










 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 



 [ATTACHMENT 03](#) 

 [ATTACHMENT 03](#) 

 [ATTACHMENT 03](#) 

 [ATTACHMENT 03](#) 

 [ATTACHMENT 03](#) 

 [ATTACHMENT 03](#) 

EnCase Forensic v7 Essentials Training OnDemand – v7.04.01i (06.06.2012), **part 3 of 3**; Note: manual broken up into three parts in order to keep attachments under 10mb for PACER.

The **Tree-Table** and the **Traeble** views are the most popular for e-mail review.

Open the **Root folder** in the outlook.ost e-mail archive.

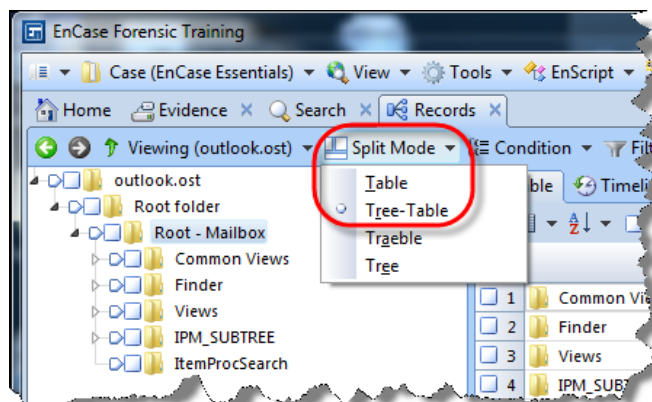


Figure 8-4 Select the mode and open Root folder

In this example, open the folder structure down to the **IPM_SUBTREE**. In Microsoft Exchange, the public folder database is divided into two trees: the IPM_Subtree and the non-IPM_Subtree. The IPM_Subtree contains folders visible to users and clients. For example, a folder created by Microsoft Outlook exists in the IPM_Subtree. A folder in the IPM_Subtree can be searched, accessed directly by users, and used to store user data. The non-IPM_Subtree contains folders not directly accessible by users, and therefore, it will not be found in an e-mail archive on workstation.¹

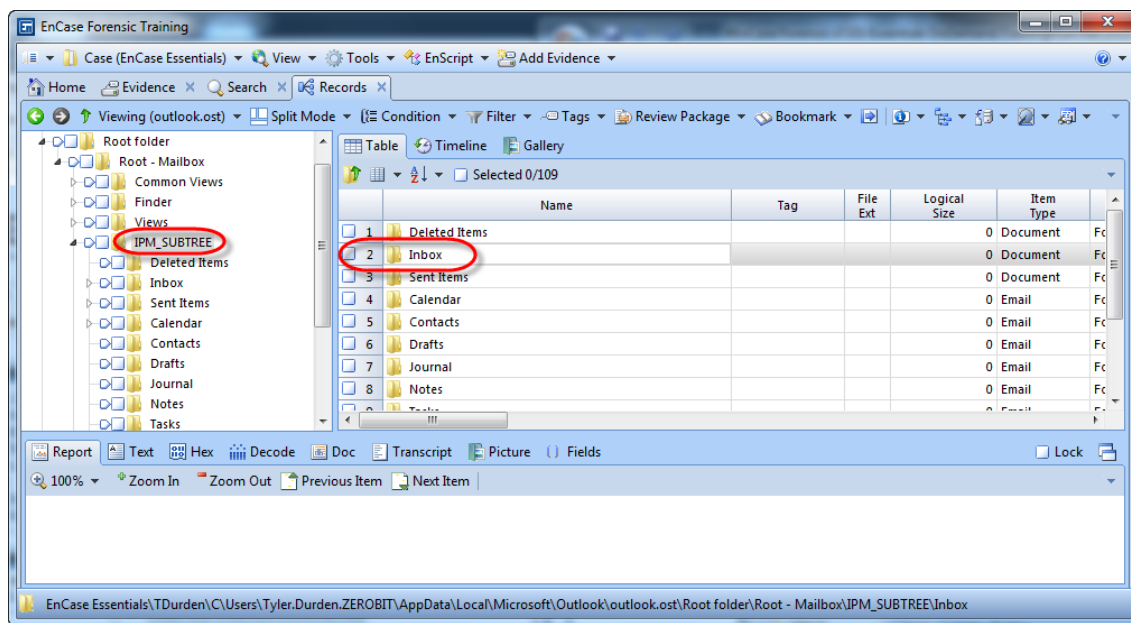


Figure 8-5 Open the IPM_SUBTREE

¹ [http://technet.microsoft.com/en-us/library/aa997291\(EXCHG.65\).aspx](http://technet.microsoft.com/en-us/library/aa997291(EXCHG.65).aspx)

You will then be able to examine the e-mail folders, including **Deleted Items**, **Inbox**, **Sent Items**, etc. As you select the e-mails, you will see the attachment icon for e-mail containing attachment(s).

In the following image, an expanded tree view of an Outlook.ost file and its folders is shown in the left pane, while the messages belonging to the .ost file are shown in the right pane, and the contents of a selected message are shown in the bottom pane.

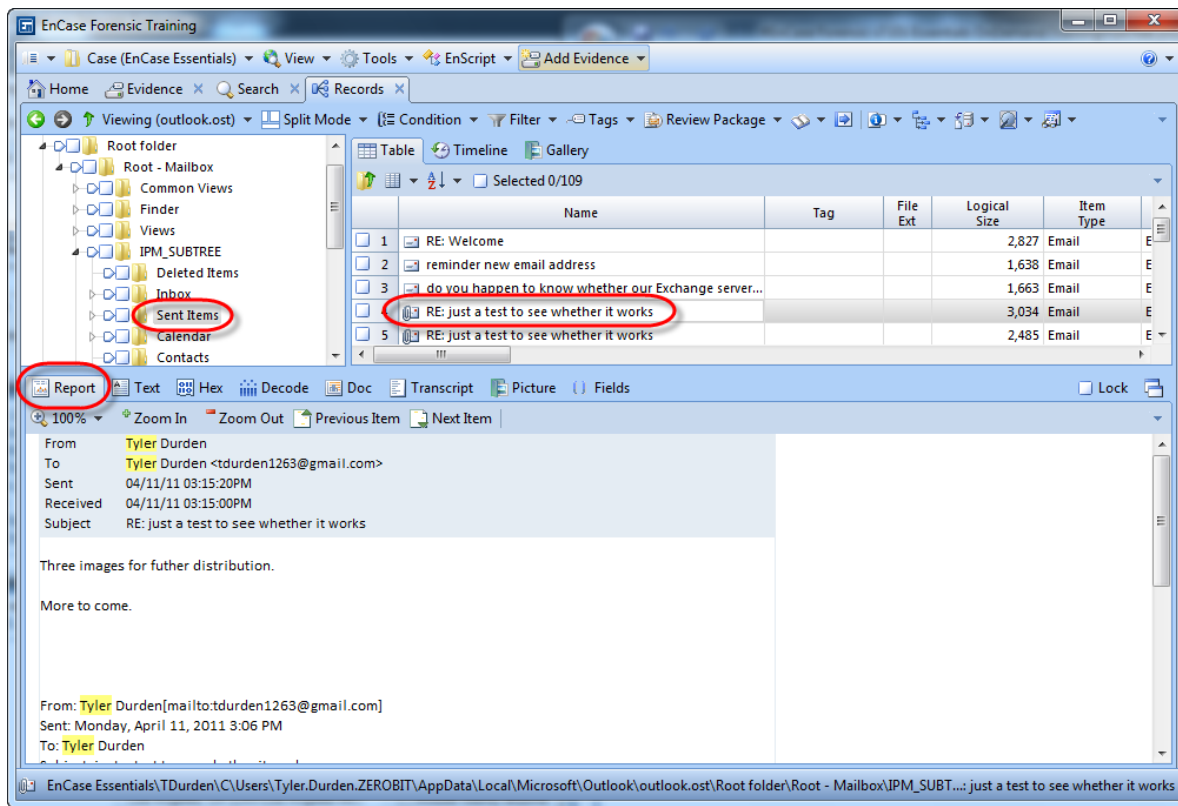


Figure 8-6 Sent Items: E-mail with attachments

You export out an e-mail message into a *.msg by right-clicking on the message and choosing **Export to *.msg...** You can also bookmark the e-mail message in the same context window.

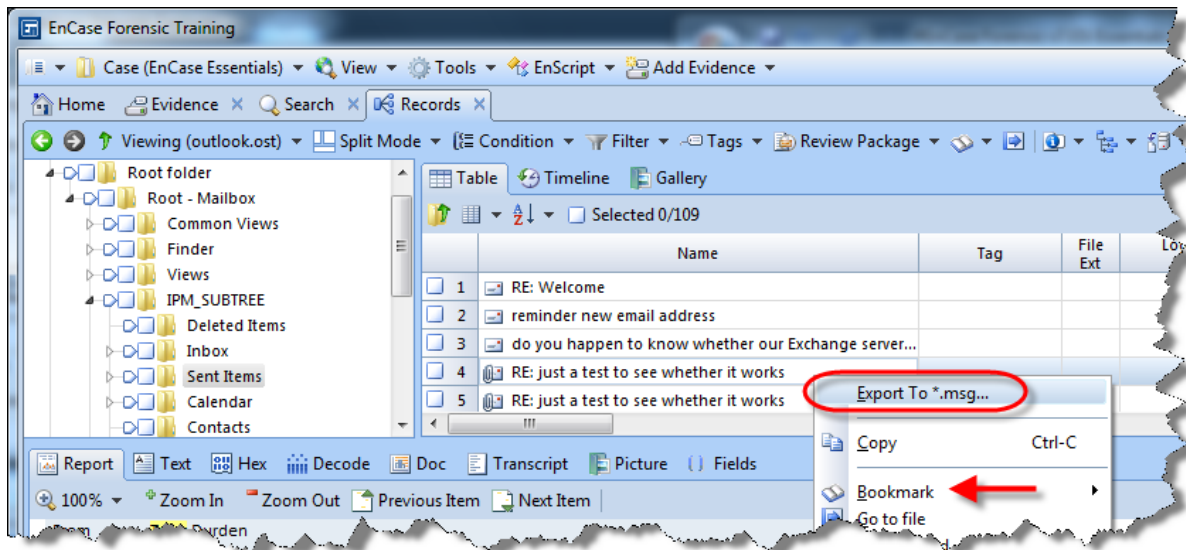


Figure 8-7 Export to .msg

You can bookmark an e-mail message as a **Single item...** or multiple e-mails at once as **Selected items...** just as you did with evidence entries.

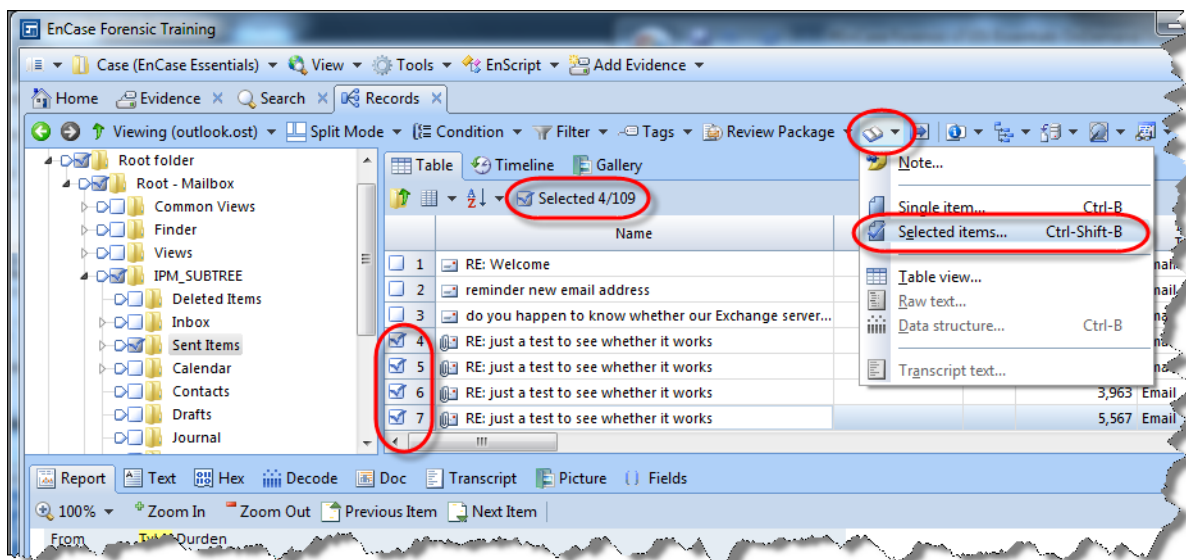


Figure 8-8 Bookmark e-mail

You can double-click on the e-mail to open it and review the attachments.

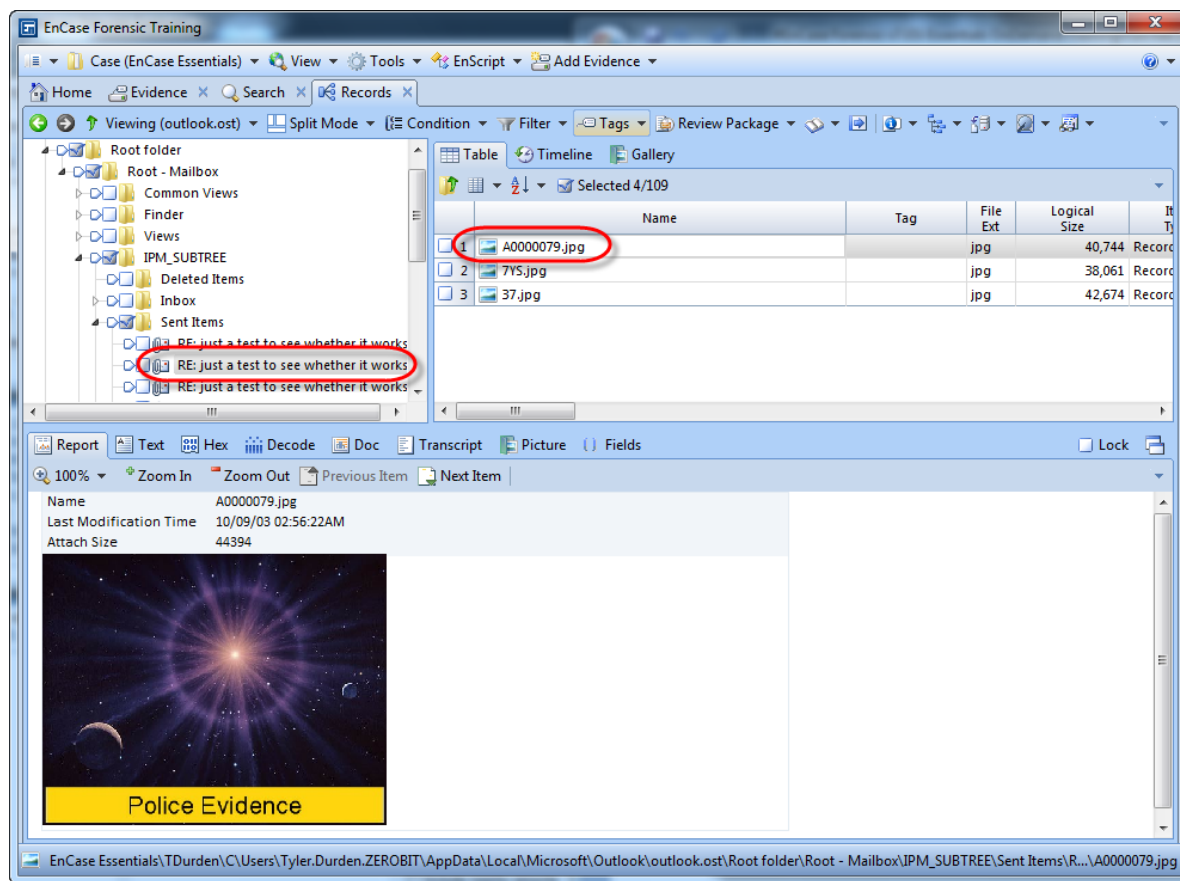


Figure 8-9 E-mail attachments

If the user has organized e-mail into subfolders, those will be available for examination.

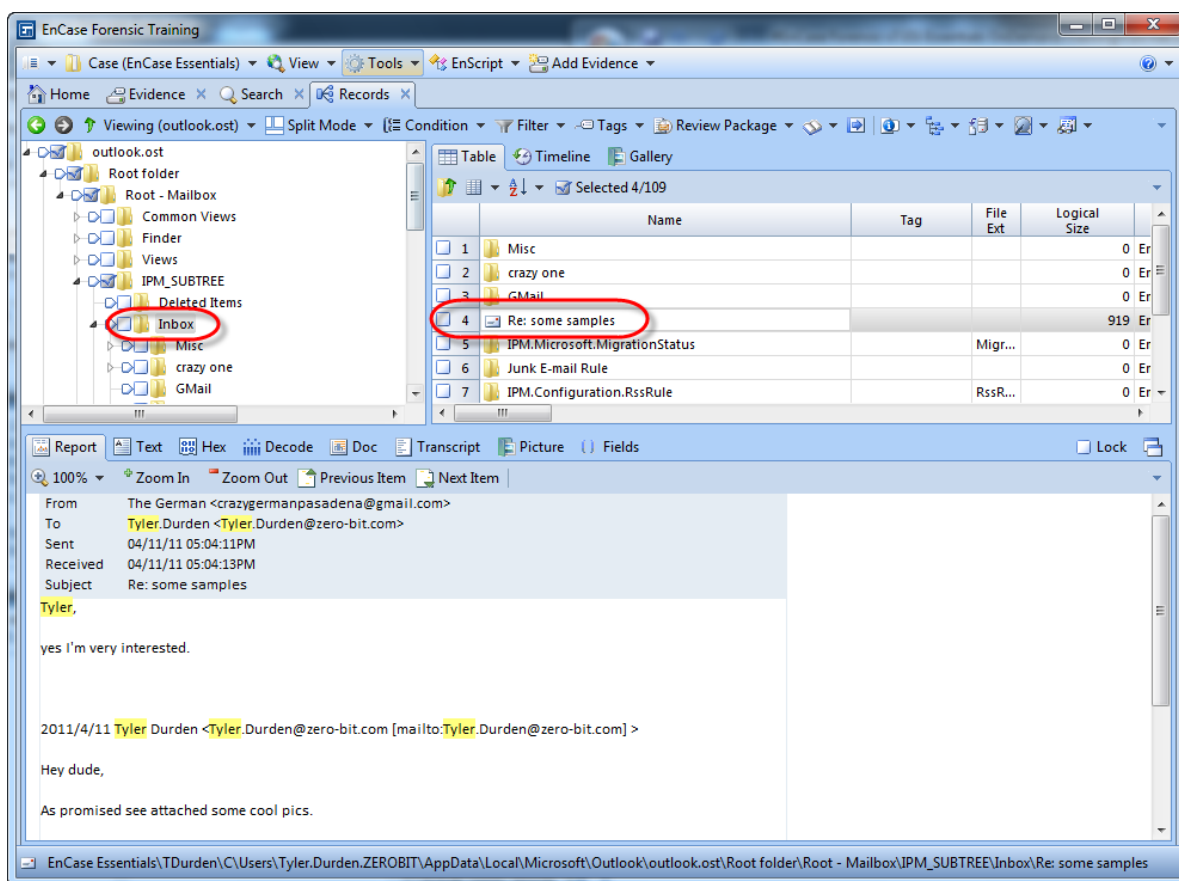


Figure 8-10 E-mail subfolders

DISPLAYING E-MAIL THREADS

EnCase v7 analyzes two forms of e-mail threading:

- Conversations
- Related messages

To choose which form of threading to examine:

1. In the Records tab, click the **Find related** menu
2. Click either the **Show conversation** or **Show related messages** button

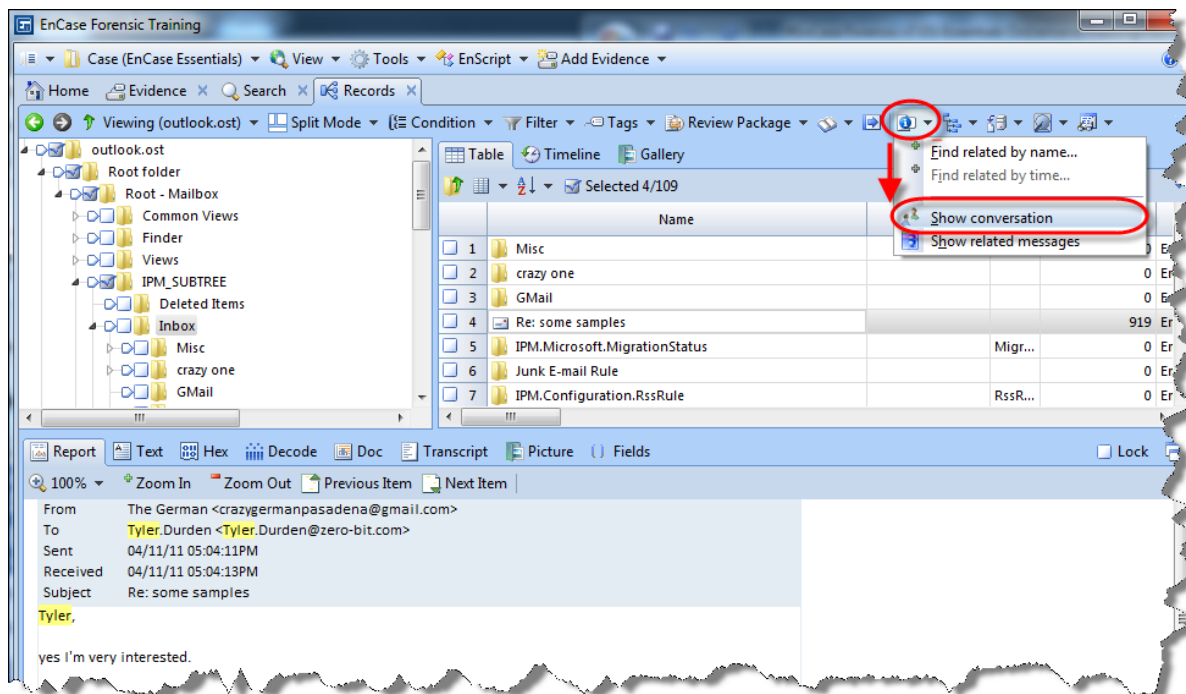


Figure 8-11 E-mail – Find Related → Show conversation

SHOW CONVERSATION

E-mail threading is based on conversation-thread related information found in the e-mail message headers.

Different e-mail systems use different methods of identifying conversations; for example:

- The header fields **Message-ID**, **Reply-To-ID**, and **References**
- The header field **Conversation Index**
- The header field **Thread-Index**
- **Multiple mechanisms** because the messages of interest cross e-mail-system boundaries. In these circumstances EnCase v7 builds a separate conversation tree for each type of data found in the header (for example, one using Message ID/References and another using Conversation Indexes) and displays the conversation tree containing the most e-mail.

EnCase v7 can display conversations for all supported e-mail types except AOL. This is because AOL messages do not store thread-related information. However the feature cannot always reconstruct complete conversations when the conversations include messages from multiple e-mail systems. For example EnCase v7 cannot fully recreate a conversation where some users are using Outlook, some are using Lotus Notes, and others Thunderbird's mbox. You can use the **Find related→Show related messages** to aid with those types of investigations.

If an e-mail does not have any of the message header fields previously specified, EnCase v7 cannot construct a conversation thread for it. Selecting such an e-mail message and clicking **Show Conversation** results in a tree containing only the selected e-mail message.

The following figure shows a conversation list for a selected e-mail (note how the e-mails contained within the conversation list are identified by their conversation index ID).

If an e-mail message references an e-mail ID that is not found, it will display as **<Message not present>**, such as shown in the following example.

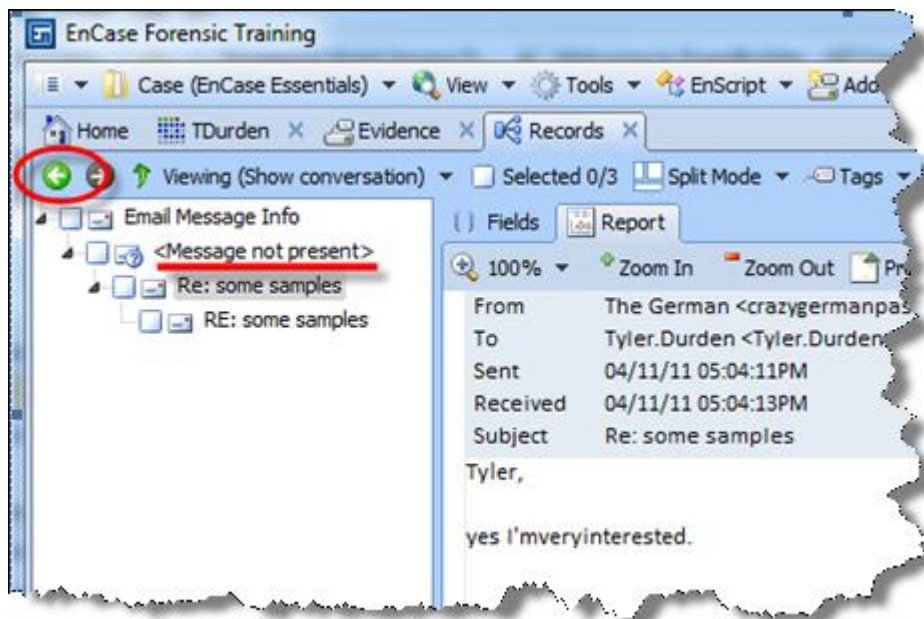


Figure 8-12 E-mail conversation

When completed, use the **Back** button to return to the e-mail archive.

SHOW RELATED MESSAGES

The **Show related messages** feature is based solely on the e-mail's subject line. The feature is useful when an examiner suspects that the **Show conversation** view is not displaying a complete conversation thread.

All e-mails with identical subject lines are considered related and displayed together.

EnCase v7 can show related e-mails for all supported e-mail types. There are no limitations caused by e-mails originating from different e-mail systems. Since the **Show related messages** view only looks at the subject line of a message, the e-mails displayed may not all be related, depending upon the uniqueness of the subject line.

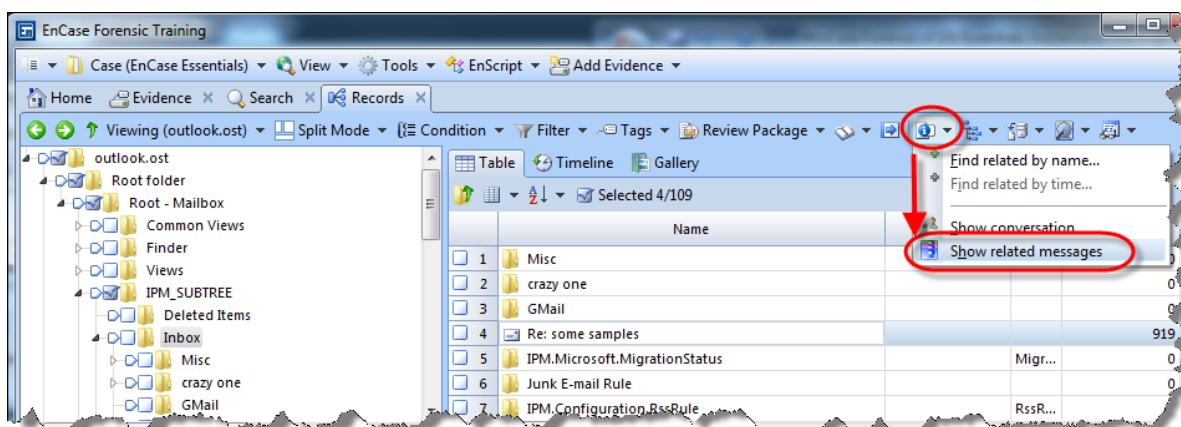


Figure 8-13 Show related messages

Following is an example of a list of related e-mails. The list is displayed in the left pane; the content of the first e-mail in the list is displayed in the Report tab.

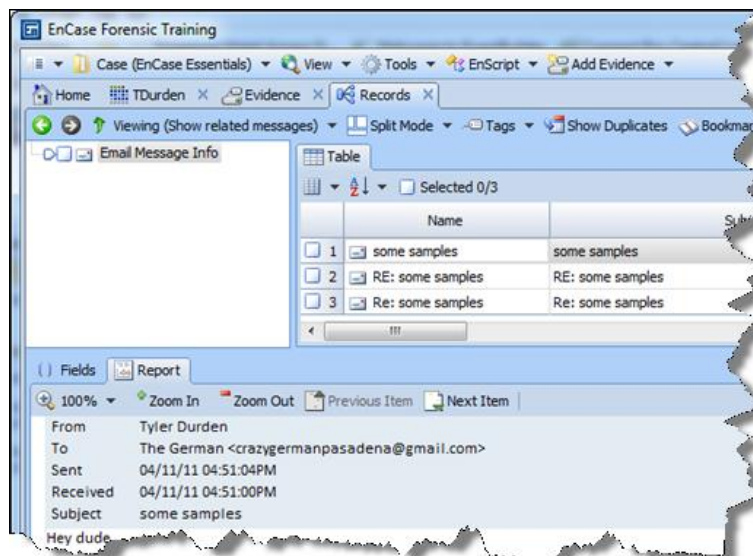


Figure 8-14 Related messages

DEDUPLICATING MESSAGES

Multiple copies of an e-mail often exist because:

- An e-mail was sent to multiple e-mail aliases
- The sender's Sent Items and the recipient's Inbox are located in a single case multiple times in different e-mail archives

By default, EnCase hides any duplicate e-mail messages in a conversation, to avoid displaying the same message multiple times, EnCase v7 deduplicates (or removes duplicates) messages in both the Show conversation and Show related messages e-mail views. The deduplication is done with the Message ID, Thread ID, or Conversation ID; depending on the type of email program.

You can now view duplicate e-mail messages in a conversation thread. To show all duplicates in a conversation, click **Show Duplicates** in the Records tab toolbar. Duplicate e-mail messages now appear with red alerts that indicate their status.

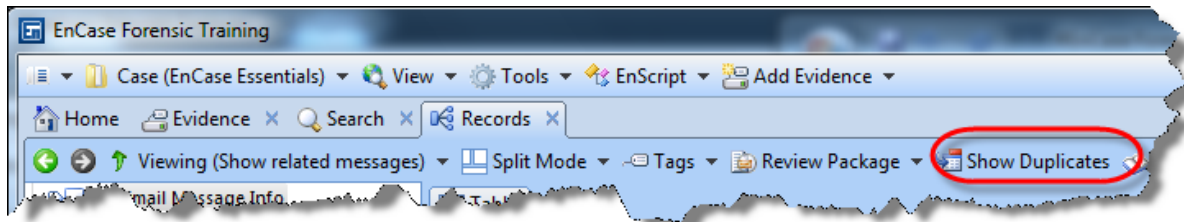


Figure 8-15 Show Duplicates

[illegible]

Bookmarking and Tagging Your Findings

BOOKMARKING DATA FOR REPORTS

As you work on a case in EnCase® v7, you typically discover files, portions of files, and other objects that are of interest as potential evidence; you can save these items for inclusion in the examination report. These marked sections are referred to as “bookmarks.” Bookmarks are saved in folders in the case file. You can view them by selecting the **Bookmarks** link under Report on the Case Home page.

Bookmarks can also contain comments and notes for tracking, accounting, and reporting purposes. You place bookmarks into bookmark folders and give them names associated with meaningful aspects of the case. The case templates that came with EnCase v7 will give you an idea of the power of bookmarks in building a report.

NOTE: If a device or compound file is removed or “dismounted” from the case file, the bookmarks and search hits that resolve within that “mounted” file will be unavailable.

To bookmark data into a folder:

1. Click the **Bookmarks** link on the Case Home page in the Reports section

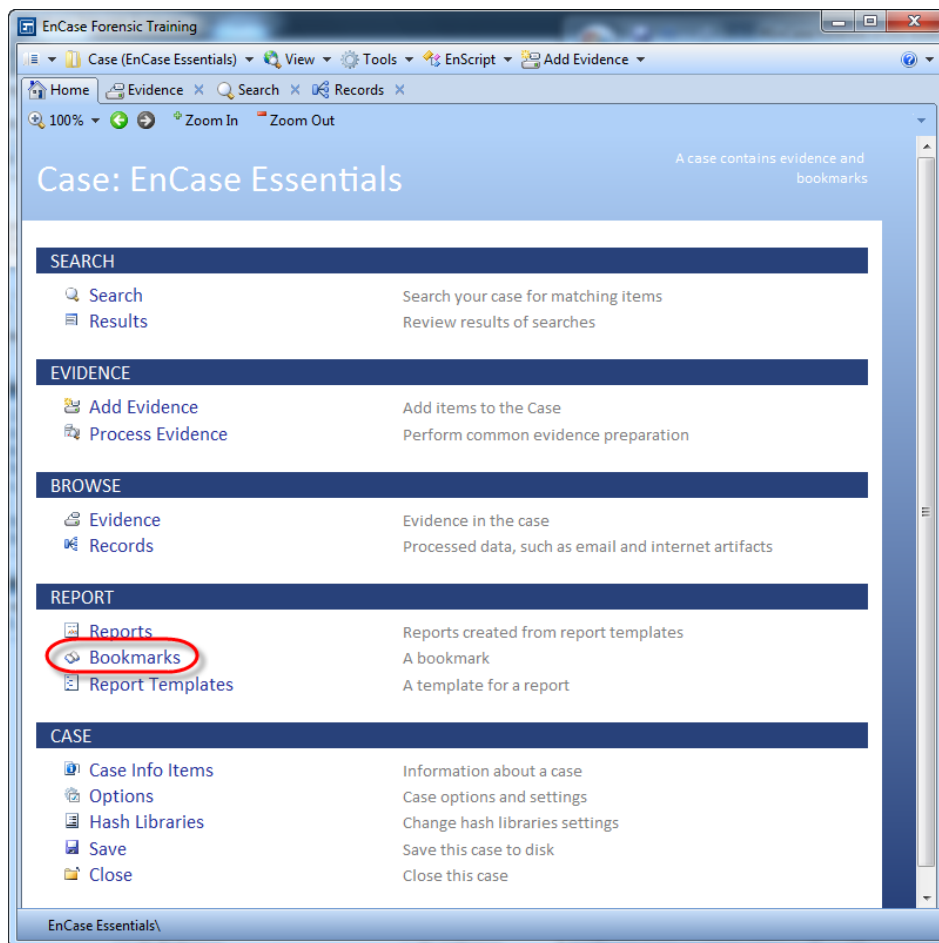


Figure 9-1 Bookmarks

2. The Bookmarks tab will open
3. Expand the Bookmarks folder to see the tree structure with the bookmarks made thus far in your examination

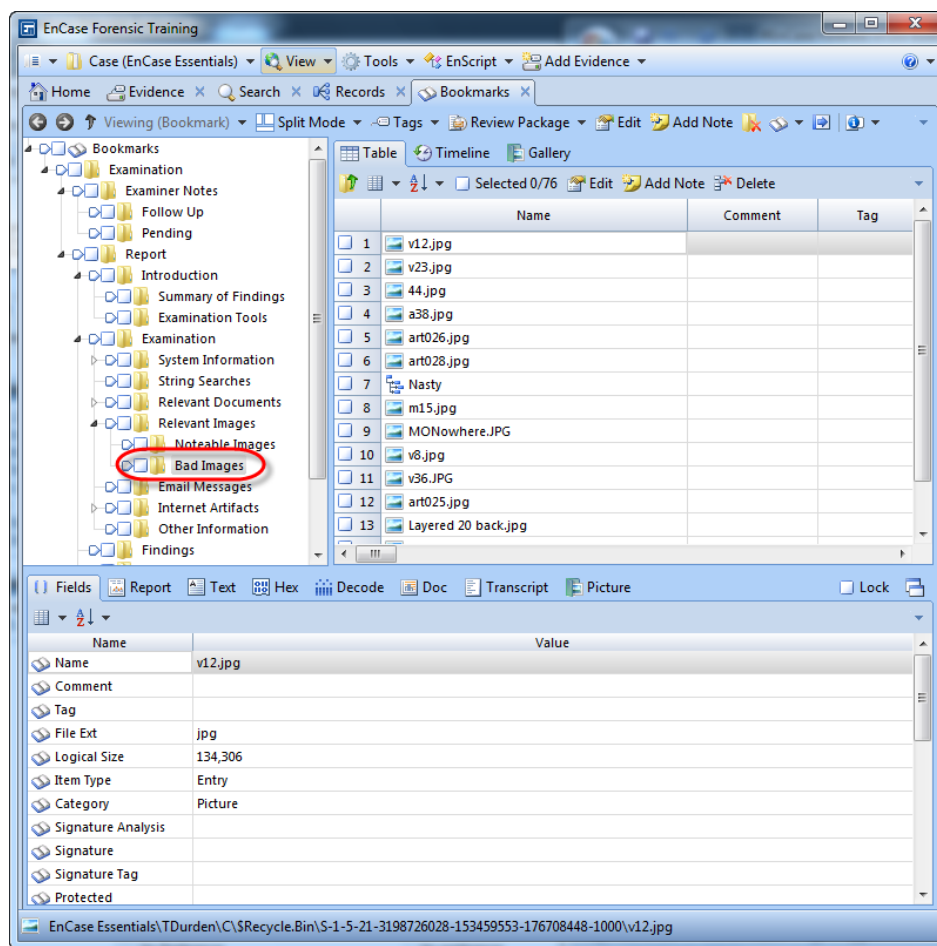


Figure 9-2 Bookmark tab

4. The case template folders will be available to hold your bookmarks and you can add any desired notes to the folders

5. You can rename, create new, or delete folders as appropriate for your case.

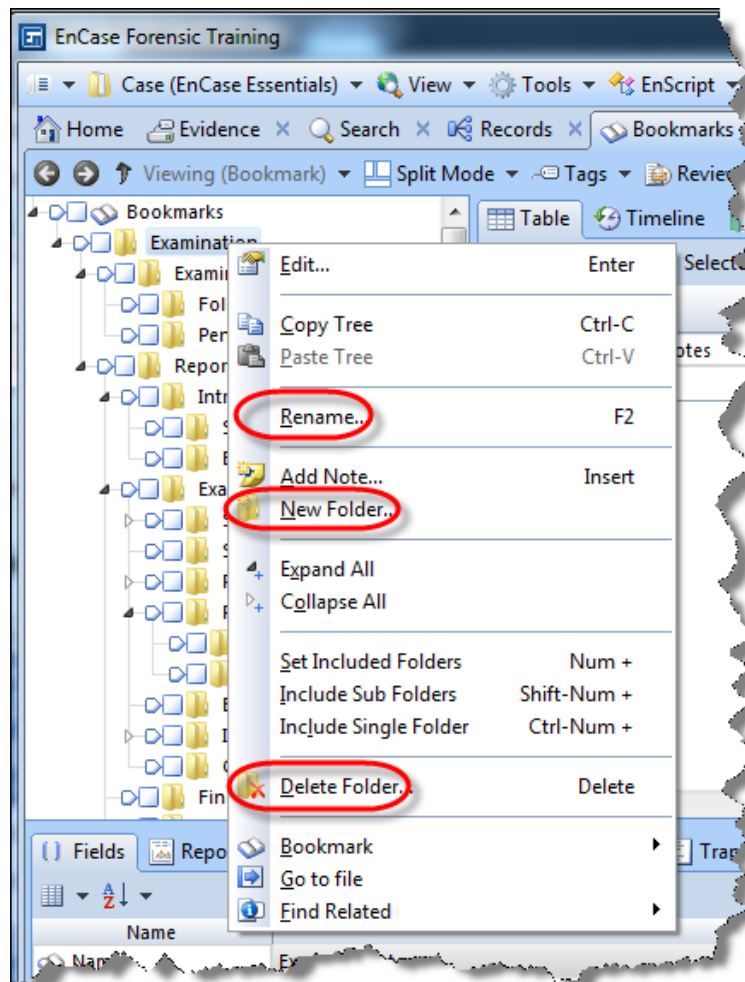


Figure 9-3 Customize Bookmark folder structure

6. As a reminder from previous lessons, to bookmark data, select the content from almost any tab and click the **Bookmark** drop-down menu on the Tab toolbar
7. Select the appropriate bookmark type (**Single File...** or **Selected Files...**), add a name and comment as desired, and click **OK**
8. View your bookmarks in the Bookmarks tab

BOOKMARKING A SINGLE ITEM

As a reminder, Single Item bookmarks are used to identify individual files that contain important information to the current case. If the file is not an image file, the contents of the file will not be bookmarked. Only the metadata information about a non-image file is displayed in the report. This type of bookmark is often used for marking non-image files that will be copied from the evidence file and placed on a CD for presentation to an attorney or case agent. It may also be used to show specific fields of important files.

Highlight the entry or record item bookmarked. Right-click on the highlighted item and select **Bookmark**→**Single item...**

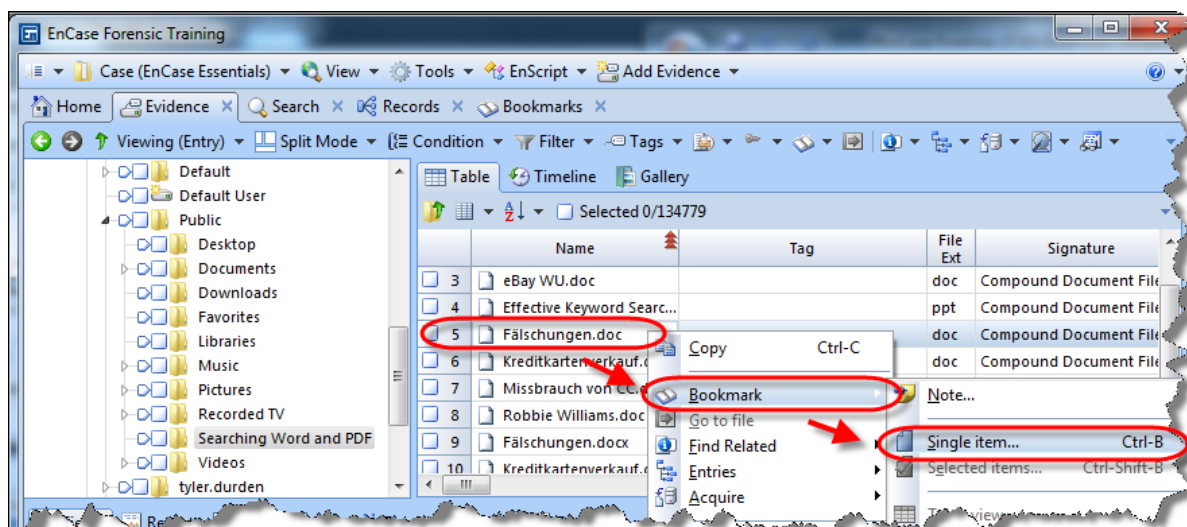


Figure 9-4 *Bookmarking a Single Item...*

You can add a comment to the bookmarked evidence and you also have the ability to use previous comments to save time.

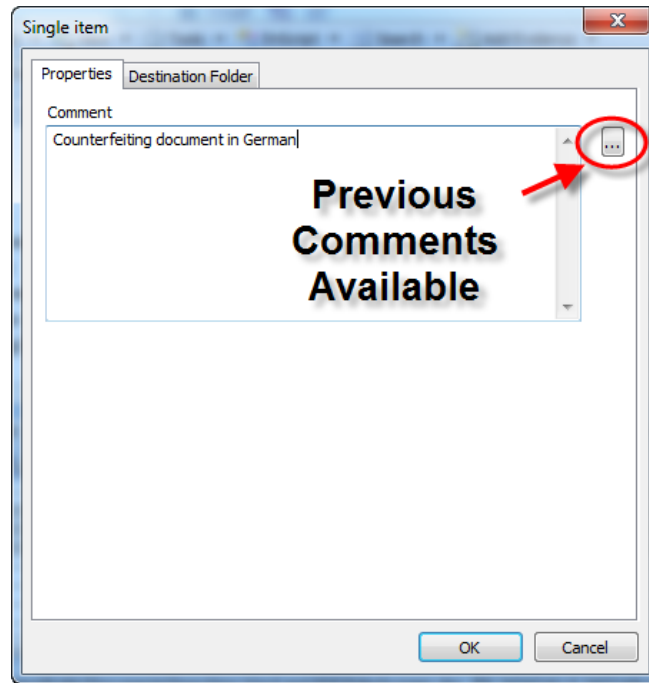


Figure 9-5 Bookmark comments

Choose the folder in the case template to add the evidence.

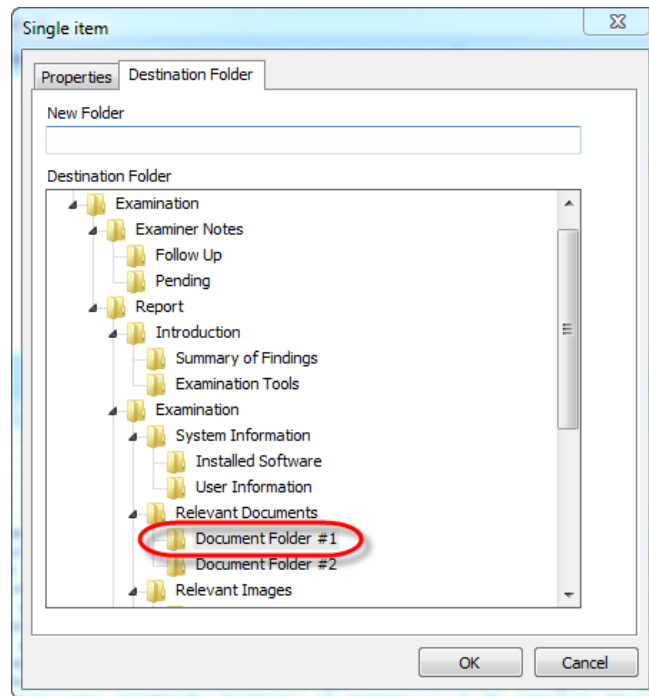


Figure 9-6 Bookmark Destination Folder

BOOKMARK MULTIPLE ITEMS

Selected Items bookmarks are similar to Single Item bookmarks except that they are used to mark a group of files not a single, highlighted file. A group of files is normally bookmarked because of some distinct quality that exists in all the selected files. It may be that all the files are images or perhaps they were all created at the same time. Another possibility is that the files are all of the same type: Accounts, checks, database files, etc.

Before beginning, ensure that no blue-check exists in the Selected box. The first step is to select the files you wish to bookmark. From the **Evidence→Viewing (Entry)** view, blue-check several files to bookmark. The Selected box will indicate how many files are blue-checked or selected. Right-click anywhere in the Table view and select **Bookmark→Selected Items...**

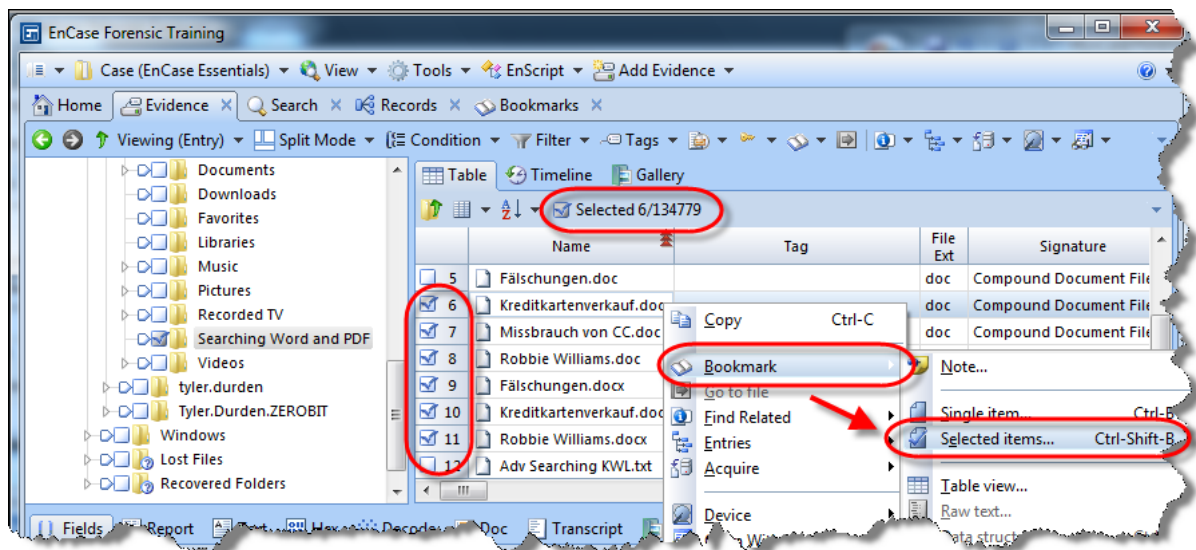


Figure 9-7 Select items to bookmark; right-click

Choose the folder in the Case Template in which to add the evidence. It will default to the last-selected folder to save time, so you don't have to select the destination folder for each bookmark.

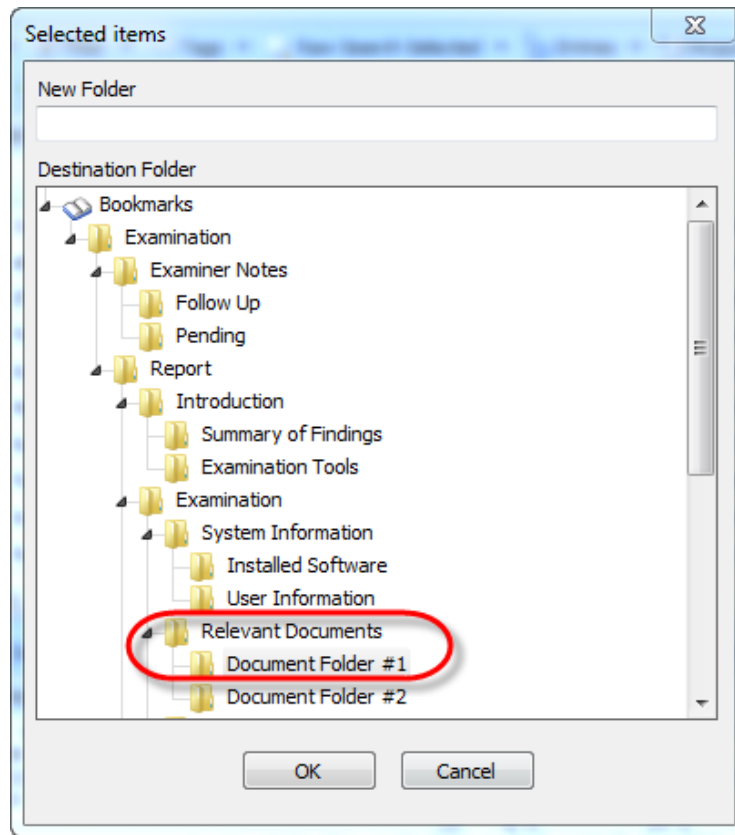


Figure 9-8 Bookmark Destination Folder

NOTE BOOKMARK

From the Bookmarks, Evidence, Record, Search Hits, and other evidentiary views, the Note Bookmark provides you more formatting flexibility than the other comment methods discussed thus far. This bookmark is designed for text data – up to one-thousand characters.

To create a Note Bookmark, right-click in the Table Pane and select **Add Note... (Insert)**.

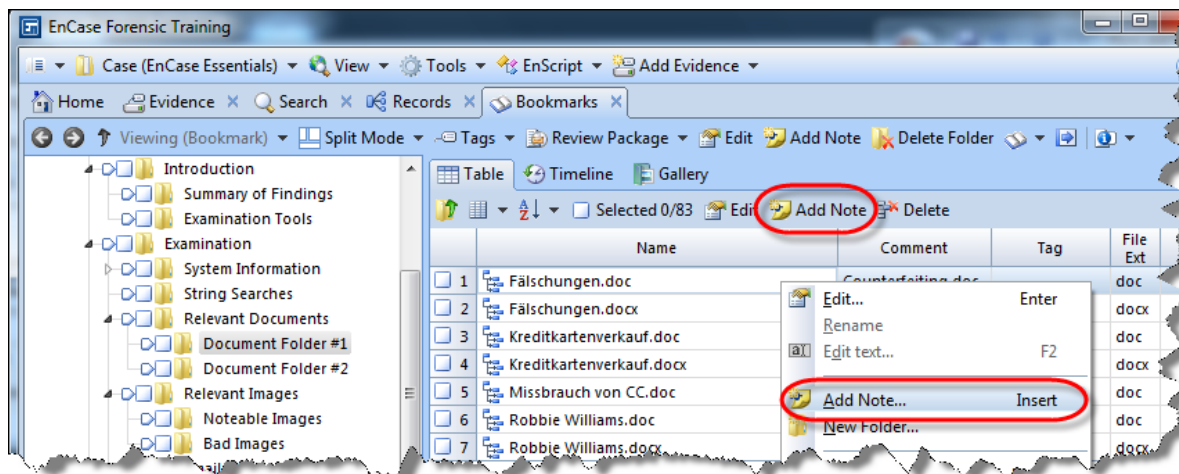


Figure 9-9 Add a Note Bookmark

Add the desired text and click **OK**.

For example, translation of the file names:

German : English

Fälschungen : Counterfeiting

Kreditkartenverkauf : Credit Card Sales

Missbrauch von CC : Abuse of CC

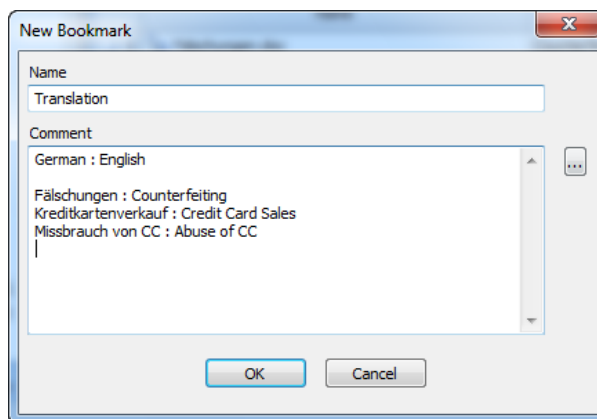


Figure 9-10 Bookmark Note

You may change the order of the bookmarks in a folder in the report. Left-click on the entry and drag the entire row to the new position.

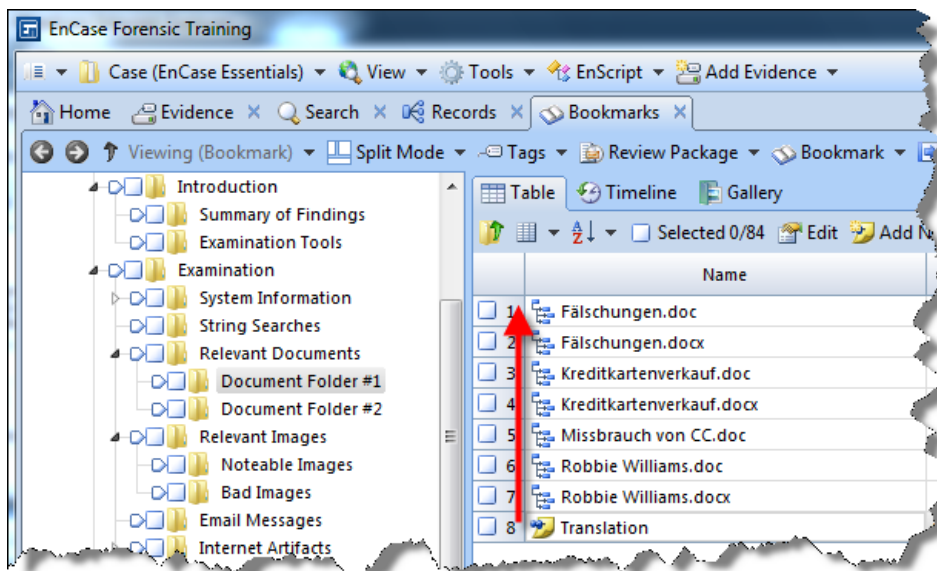


Figure 9-11 Rearranging bookmarks

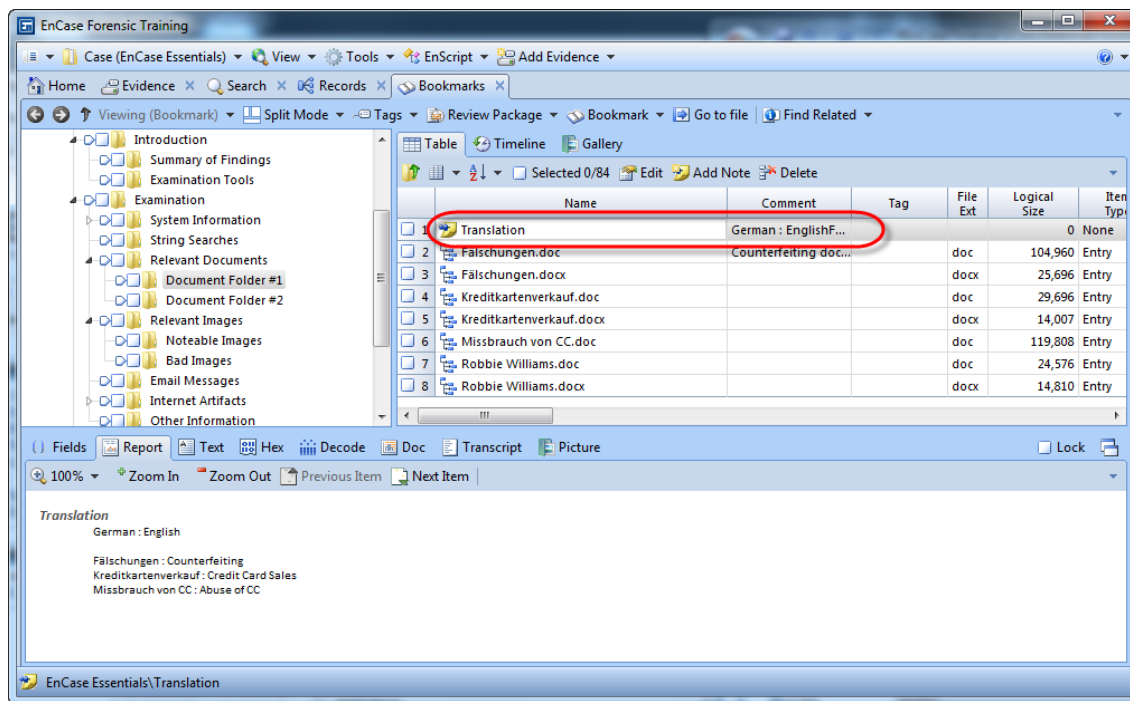


Figure 9-12 New order of Bookmarks

You can rename the folder (F2), reorder folders, add new folders, and arrange the examination report as appropriate.

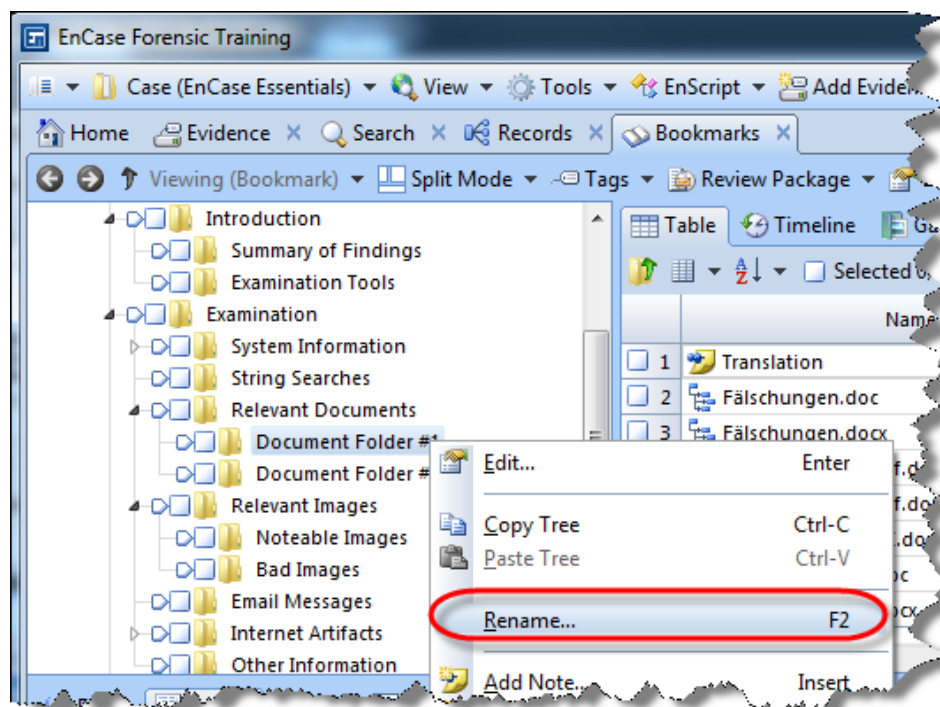


Figure 9-13 Rename the folder

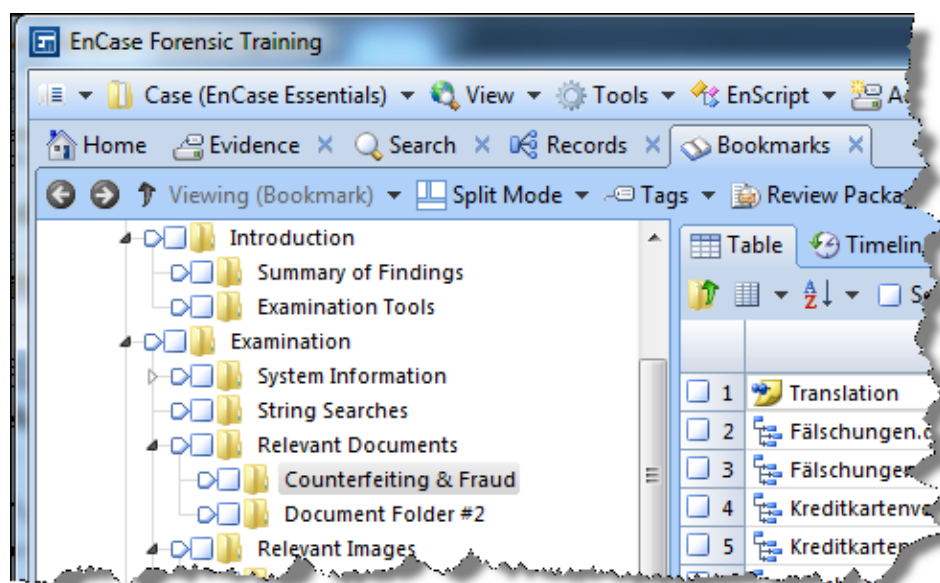


Figure 9-14 Renamed folder

TAGS

The EnCase v7 tagging feature allows you to mark evidence items for review. You define tags on a per-case basis, and default tags can be part of a Case Template.

Any item that you can currently bookmark can also be tagged. You can search for tagged items, view them on the Search Results tab, and view the tags associated with a particular item in an Evidence or Records table.

Following is a list of tag features and characteristics:

- You can create tags as part of a case or add them to a Case Template. You can customize each of the tags with specific colors and display text.
- You can edit saved tags: change their colors and text, hide specific tags from viewing, and delete a tag.
- Tags are local to a specific case (that is, you cannot create global tags), and the maximum number of tags that you can use for a case is 63.
- You can directly manipulate tags on the EnCase® user interface: change their order, delete them, and so forth.
- You can modify the order in which tags are displayed in the Tag column.
- Once you have created a tag, you can build searches based on tags and also tag search results. You can also combine tags with index and keyword search queries.
- You can create tags using EnScript modules.

CREATING TAGS

To create a tag:

1. From the Records, Evidence, or Bookmark tabs, click **Tags** on the toolbar

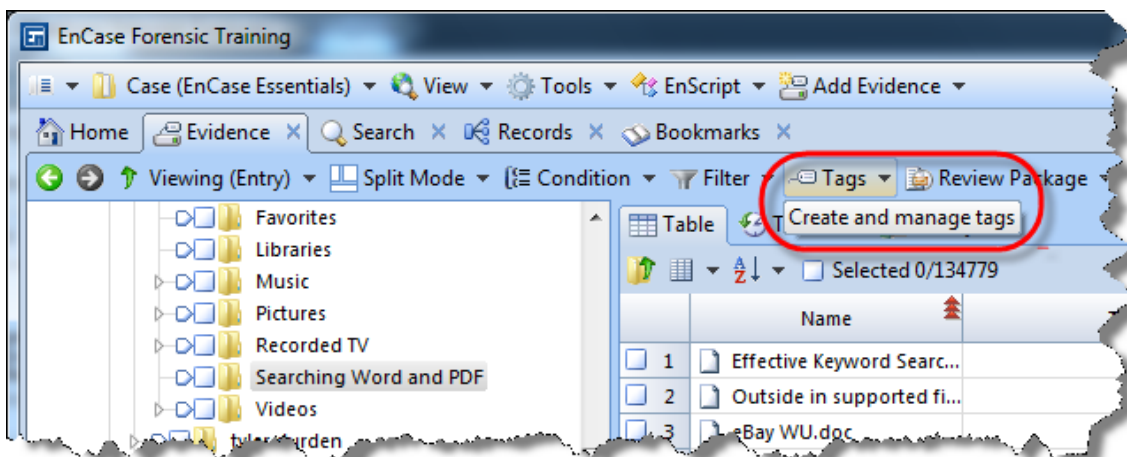


Figure 9-15 Creating a tag

2. On the Tags drop-down menu, click **Manage Tags...**

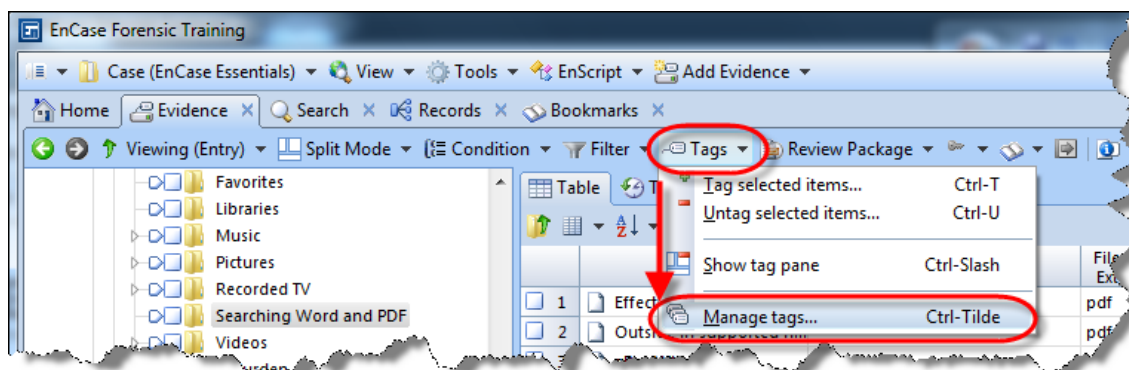


Figure 9-16 Tag menu

3. Sample tags are available for you to utilize as appropriate to your case, such as:
- **Review** – Review later as time permits
 - **Add to Report** – Reminder to add to the report
 - **Follow Up with Submitter** – Entry or recording requiring follow-up discussion or review with the person submitting the evidence for analysis
 - **Ignore** – Already reviewed and not relevant to the current investigation
4. If you wish to add additional tags, click **New** from the **Manage Tags** toolbar

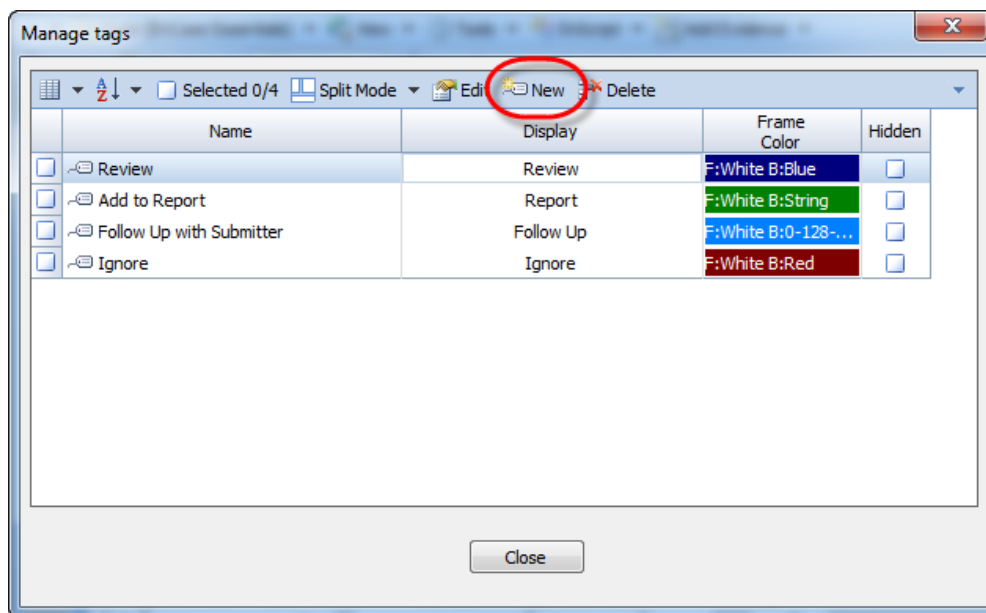


Figure 9-17 Manage tags

5. On the New Tag Item panel, enter a **Name**, the **Display** text that you want to appear in the tag column (use short display names to conserve space in the column), and the **Frame Color** (foreground and background colors) for the tag; you can also hide or disable the tag by checking its **Hidden** box
6. In this example, you can create a tag for images depicting apparent minors engaged in sexually explicit conduct for submission to the National Child Victim Identification Program

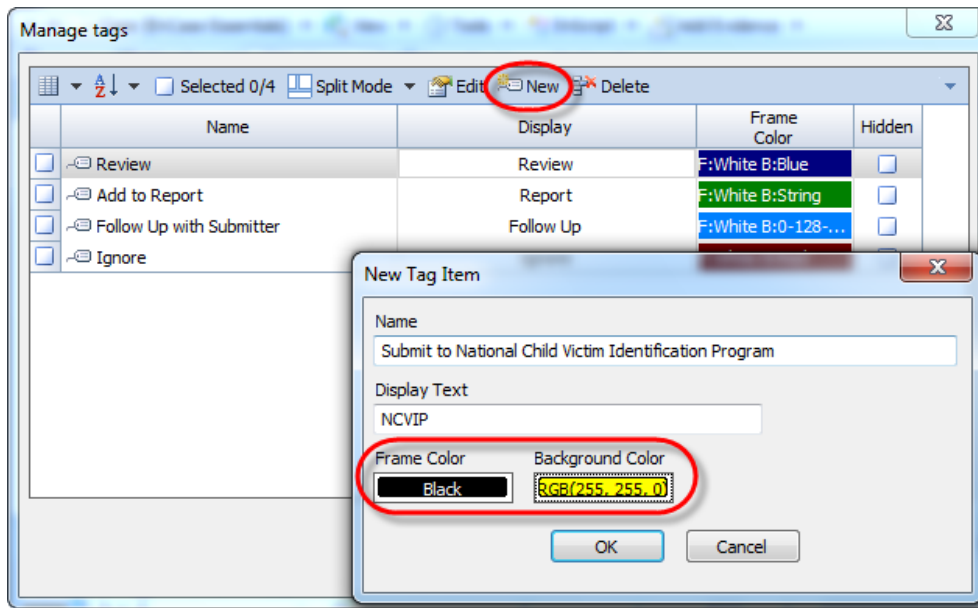


Figure 9-18 New Tag Item

7. Repeat the steps until you have created the tags you want; you can always add, remove, and rename tags later

8. Click **OK** and the tag will now be available for your case work

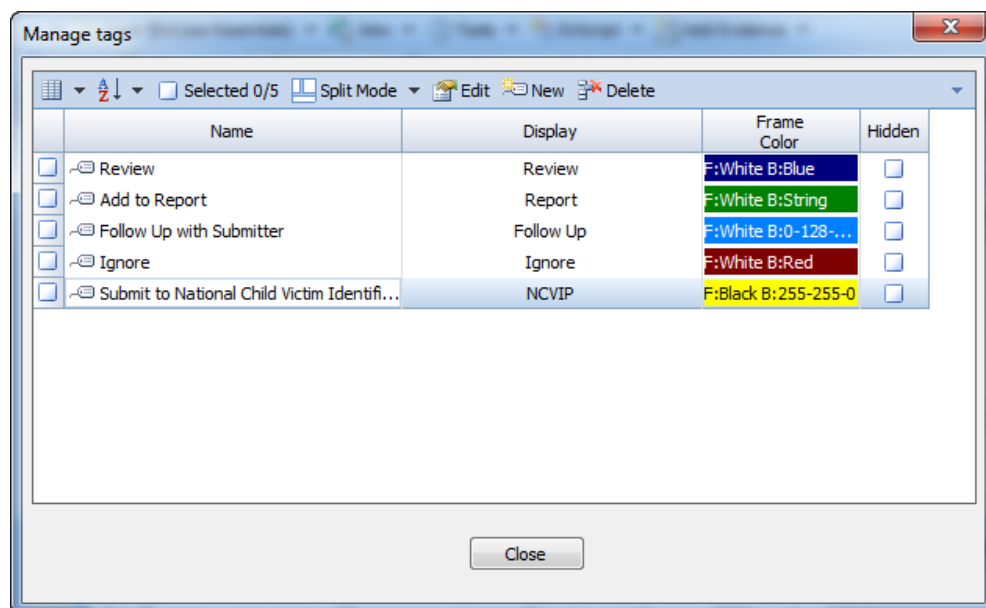


Figure 9-19 New tag

At anytime you can display a list of available tags by clicking **Tags→Show tag pane**. You can use this to toggle the Tag pane on and off.

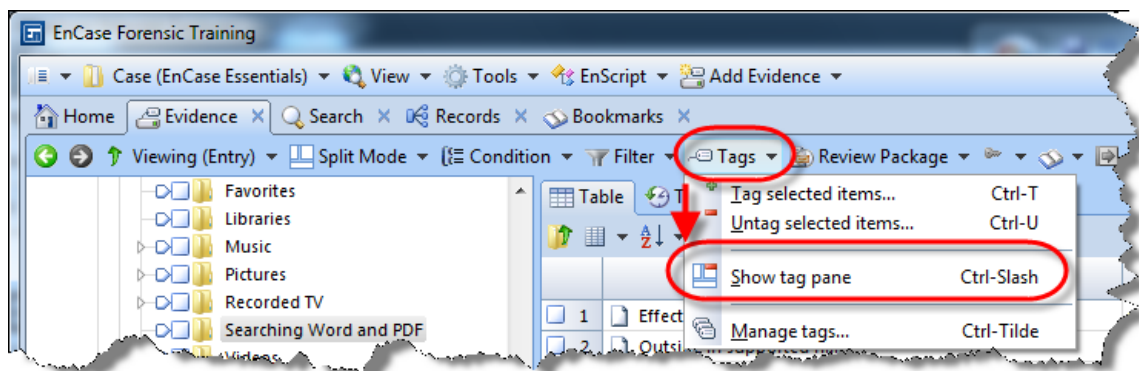


Figure 9-20 Show tag pane

The Manage tags pane will appear in the bottom right corner to assist you in your tag management.

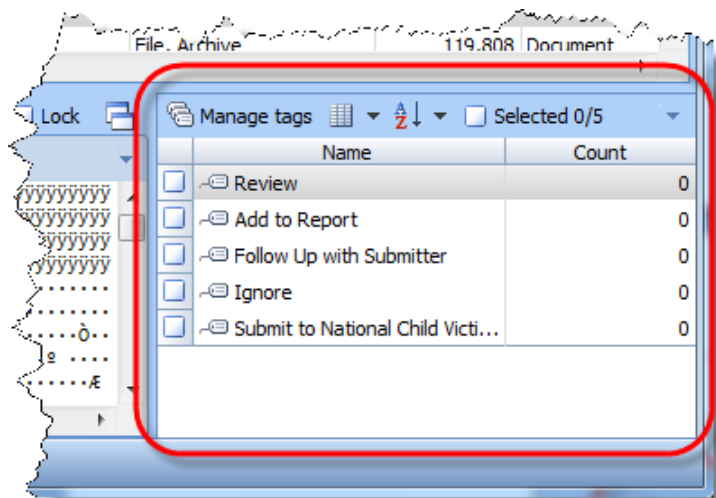


Figure 9-21 Manage tags pane

TAGGING MULTIPLE EVIDENCE ITEMS

You can tag multiple files at once.

Blue-check the selected items and then select the **Tags** menu, choosing **Tag selected items...** (**Ctrl-T**).

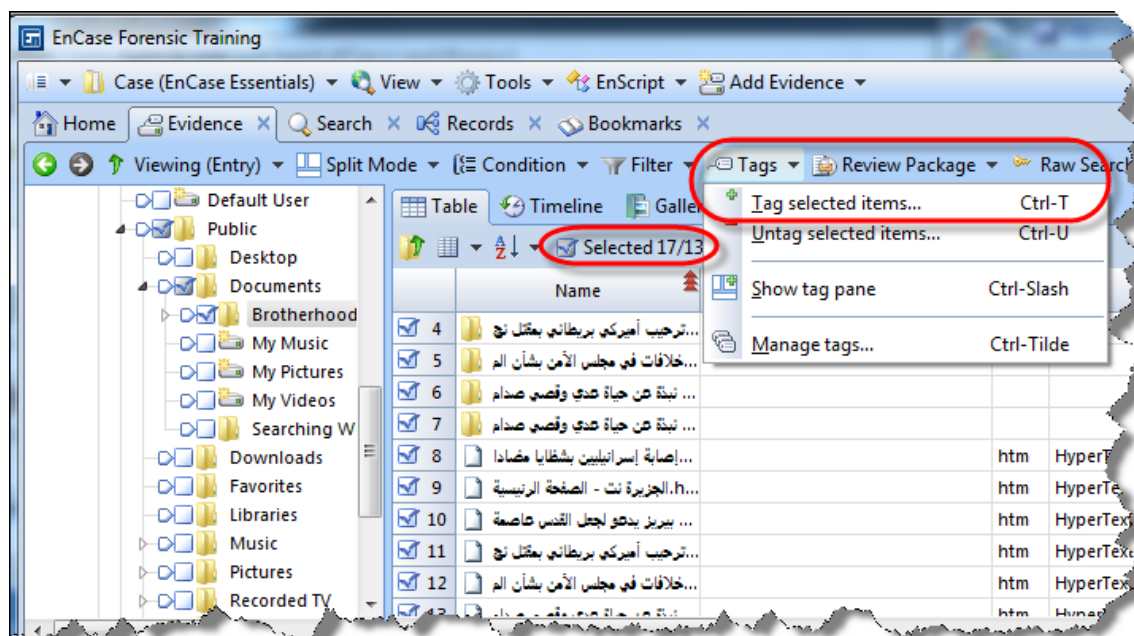


Figure 9-22 Tag selected items...

Choose the tag you wish to apply to the evidence items.

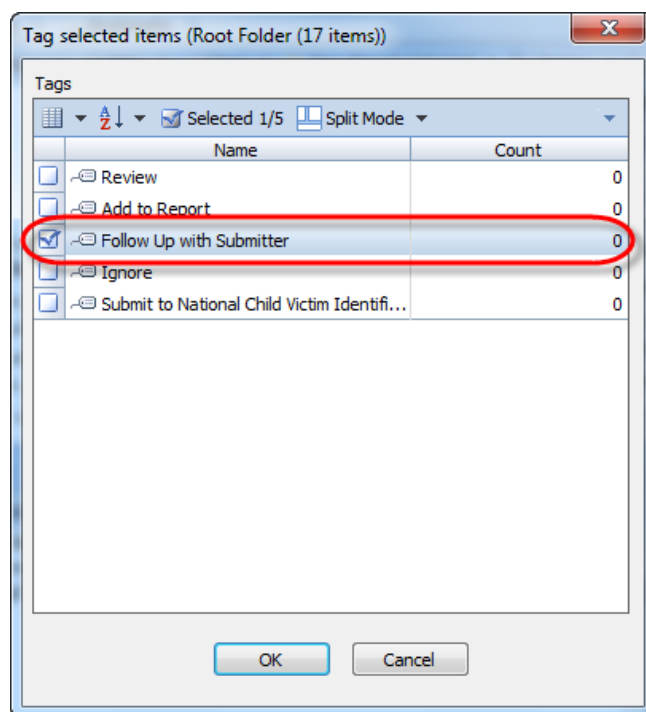


Figure 9-23 Tagging selected items...

The evidence items will have the tag displayed in the Tag column of the Table Pane.

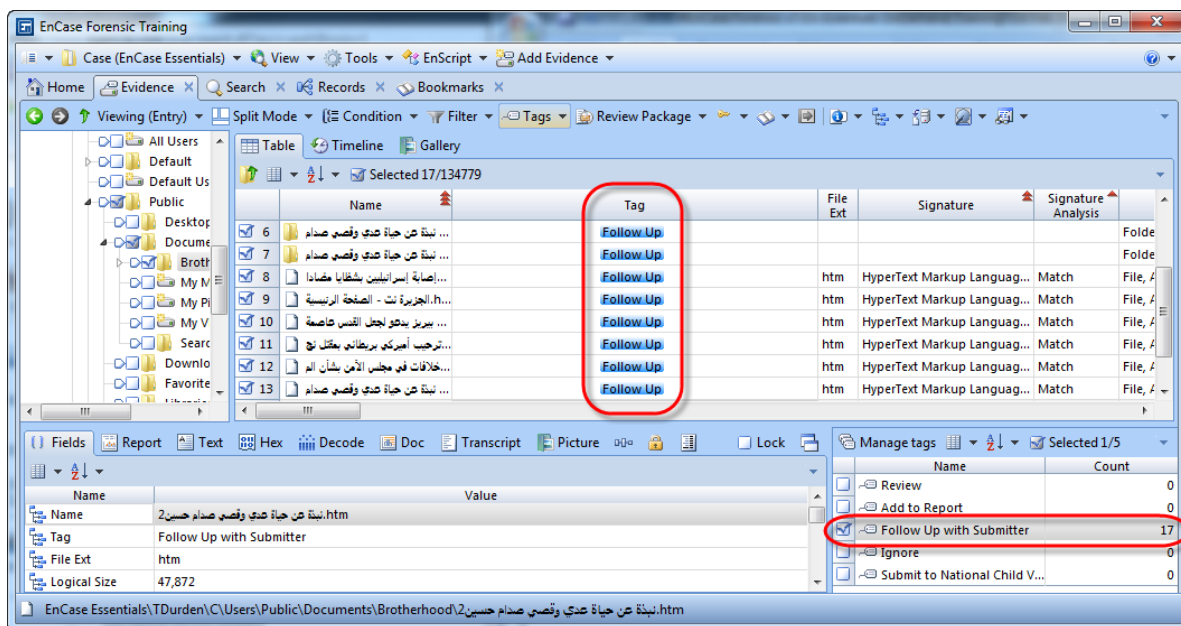


Figure 9-24 Tagging selected items

USING THE TAG PANE AND COLUMN

Another method of tagging is to use the Tag Pane. To tag an evidence item, do the following:

1. Your evidence items are available on the Evidence tab; you can also assign tags to Records and Bookmarks
2. Select the evidence item to be assigned a tag by highlighting or checking it
3. Check the tag that you want to assign to an evidence item (this example uses the new tag you created)

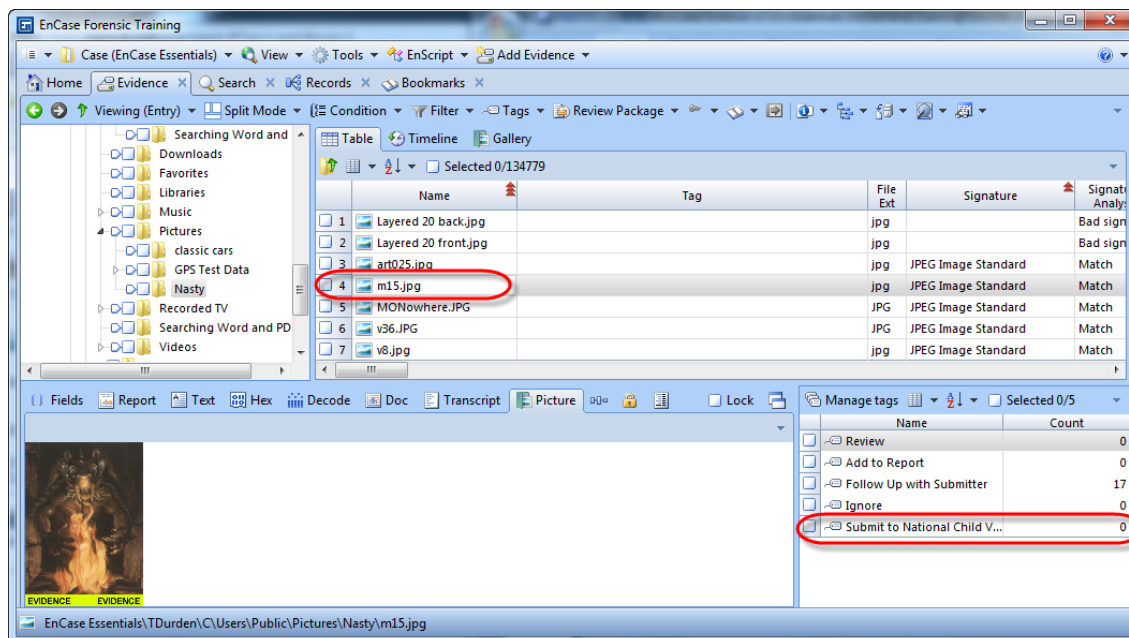


Figure 9-25 Select the tag for the evidence item

4. The tag you selected appears in the Tag column of the selected evidence item

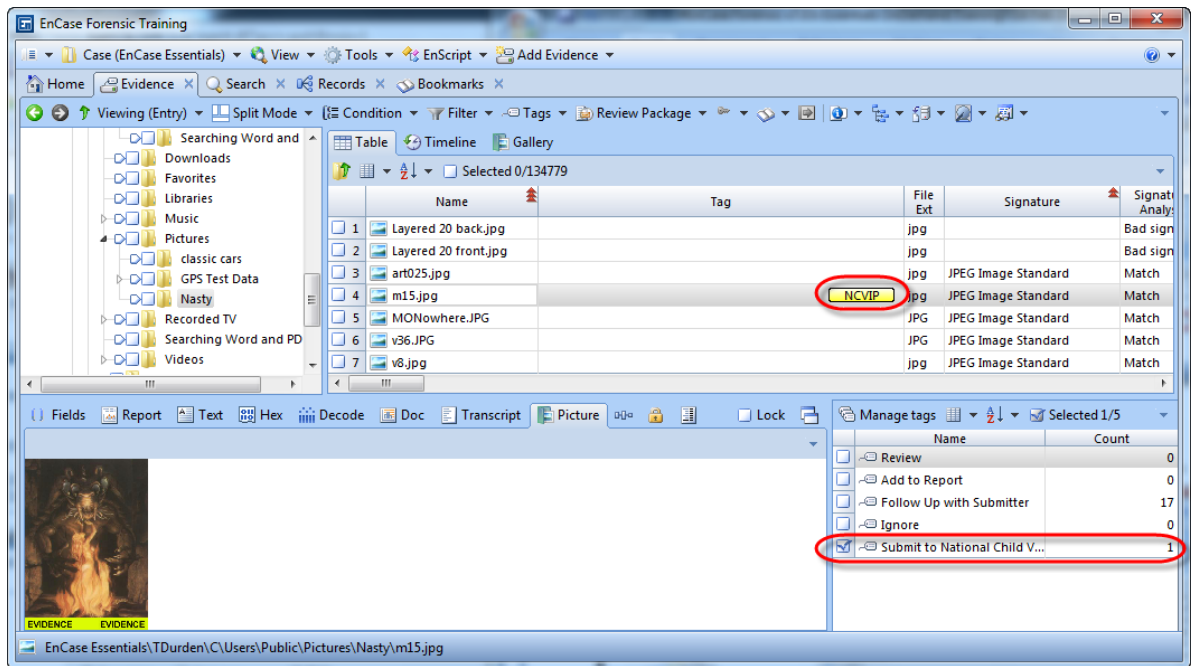


Figure 9-26 Tag in Table view

One-click Tagging

You can also set a tag by clicking on its position in the Tag column.

1. To set a tag using the Tag column, click the space in the Tag column where the tag would be displayed and it will then appear
 - As an example, if you have two tags configured, half of the column will be used to display the first tag and the second half of the column will be used to display the second tag
 - If you click in the first half of the tag cell for the item you wish to tag, that will apply the first tag to that item and it will now appear in the column
 - To remove a tag, simply click the tag in the column

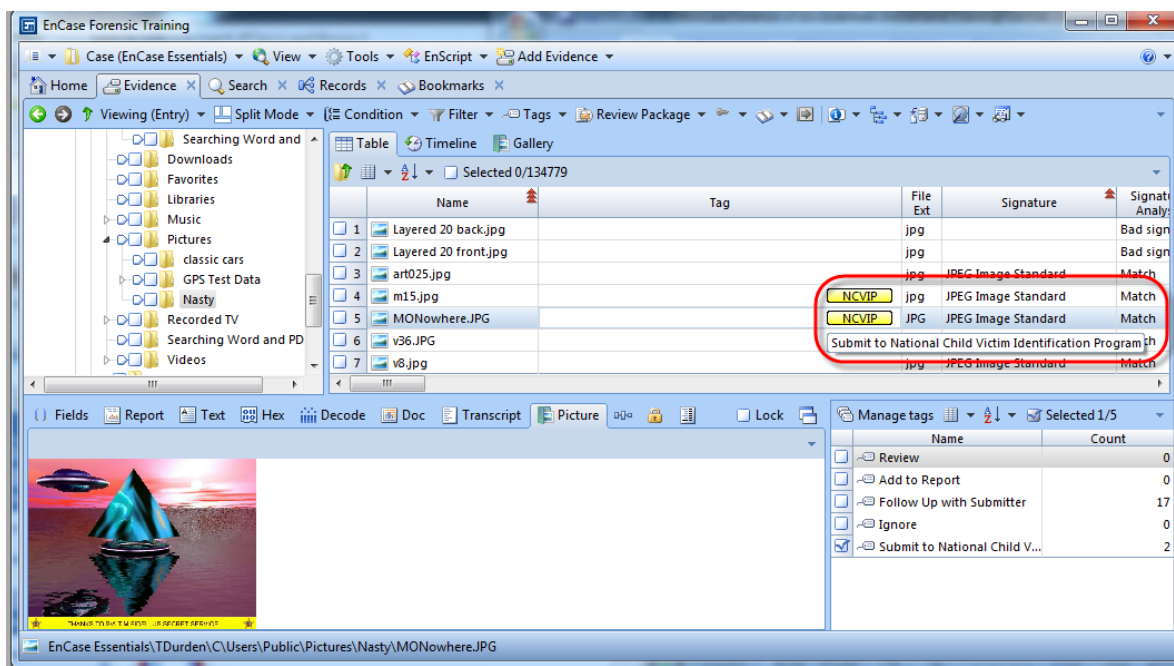


Figure 9-27 Tagging with a click

You can change the order of the tags on a row by clicking on a tag and dragging it in the Tag pane.

TAGGING IN THE SEARCH VIEW

In the Tags tab of the Search view, you can find tagged data to quickly review items that have been flagged for special attention. Clicking in the **Tag** column in the Table Pane automatically adds or removes a tag from that item.

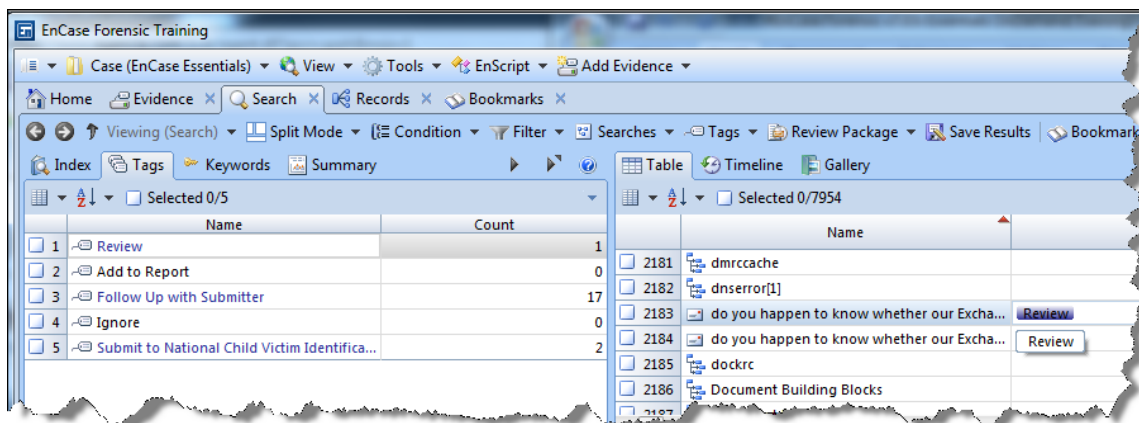


Figure 9-28 Tagging with a click – Search View

HIDING A TAG

If you have a tag that you do not currently want to show in the Tag column or the Tag pane, you can hide the tag using the options available from Manage tags window. This will not delete a tag, but will simply hide it from view.

To hide a tag, follow these steps:

1. From the Evidence tab, click the **Tags** button
2. In the Manage tags dialog, check the box in the **Hidden** column for the cell corresponding to the tag you want to hide

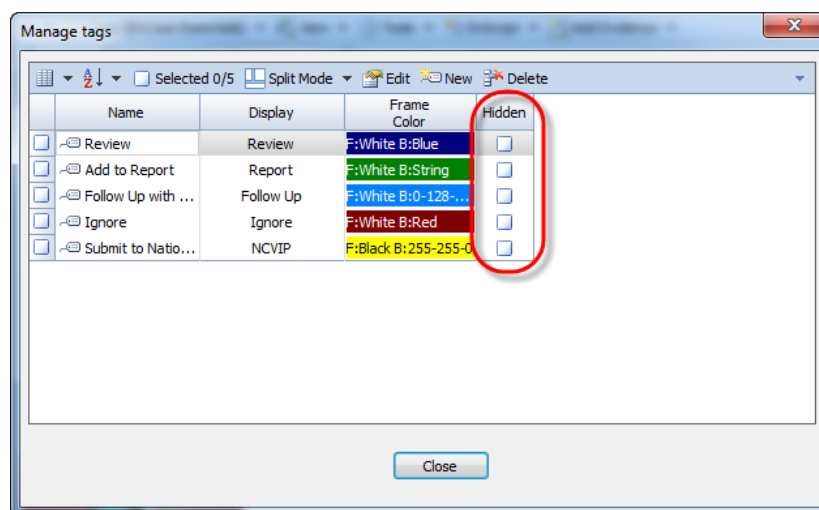


Figure 9-29 Hiding a tag

DELETING TAGS

Tags that you do not want to use can be deleted from the Manage tags window. Deleting a tag removes the tag name from the case, and deletes all references to the tag in the tag database. *This action cannot be undone.*

When deleting a tag, if that tag has been assigned to an item in the case, a warning dialog will indicate the number of tags to be deleted. If no items are tagged with that tag name, then no warning will be displayed.

To delete a tag, follow these steps:

1. On the Evidence tab, click the **Tags** button
2. On the Manage tags dialog, check the row containing the tag that you want to delete
3. On the Manage tags toolbar, click **Delete**

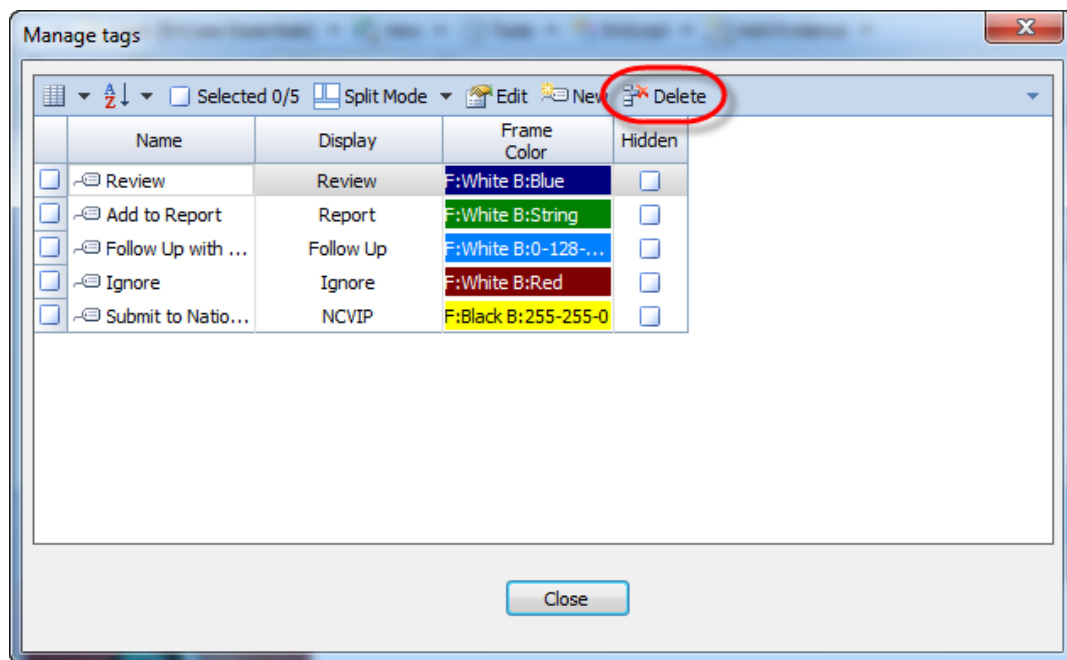


Figure 9-30 Deleting a tag

[illegible]

Reporting

The final phase of a forensic examination is reporting the findings, which must be well-organized and presented in a format that the target audience will understand. EnCase® v7 has added several enhancements to its reporting capabilities that strengthen this phase of the process. These include:

- The additional of reporting templates that you can use as is or adjust to suit your needs
- The capability to control a report's format, layout, and style
- The ability to add notes and tags to a report

Reports in EnCase v7 consist of two parts:

1. Report templates that hold the formatting, layout, and style of the report.
2. Bookmark folders where reference to specific items and notes are stored. The Report template links to bookmark folders to populate content into the report.

USING REPORT TEMPLATES

A report template is one component of a case template. Each of the default case templates has a customizable report template included. Different case templates may contain different report templates, and each of these templates is completely customizable. In addition to the report template, each case template also includes bookmark folders that are referenced in the report.

Besides the default templates, you can define your own custom reports and save them as part of a case template.

EnCase v7 includes the ability to create reports from additional metadata fields for entries and records. The report template builder makes all evidence fields available and, if selected, the field values display in the report.

You can customize reports by specifying which fields to add to the report template. To add a field, select it from the report fields available. You can choose to include the value in the field as well as the name of the field. Then, when you generate a report, EnCase v7 includes both selected fields and the content with which they are populated in the specified area of the report.

All entry, record, and item (bookmark) fields can be added to report templates. Multi-value fields, such as file extents and permissions, have two options for inclusion: cell and table. Adding the cell data displays the value of the field as displayed within the Entry table view. Adding the table data displays the value of the field as displayed in the **Details** tab.

Report Template Structure

Before viewing a report, you need a report template or outline of what the report will look like. The report template also defines how your case data is formatted and styled. This structure consists of:

1. **Report Sections** – Sections contain groups of like information and formatting and provide the ability to organize your report
2. **Report Formatting** – This includes page layout, section design, and text styles
3. **Report elements** – Collections of bookmarks, a key element of the report structure (you do not embed bookmarks into a report template, but embed a *reference* to the contents of a bookmark folder)

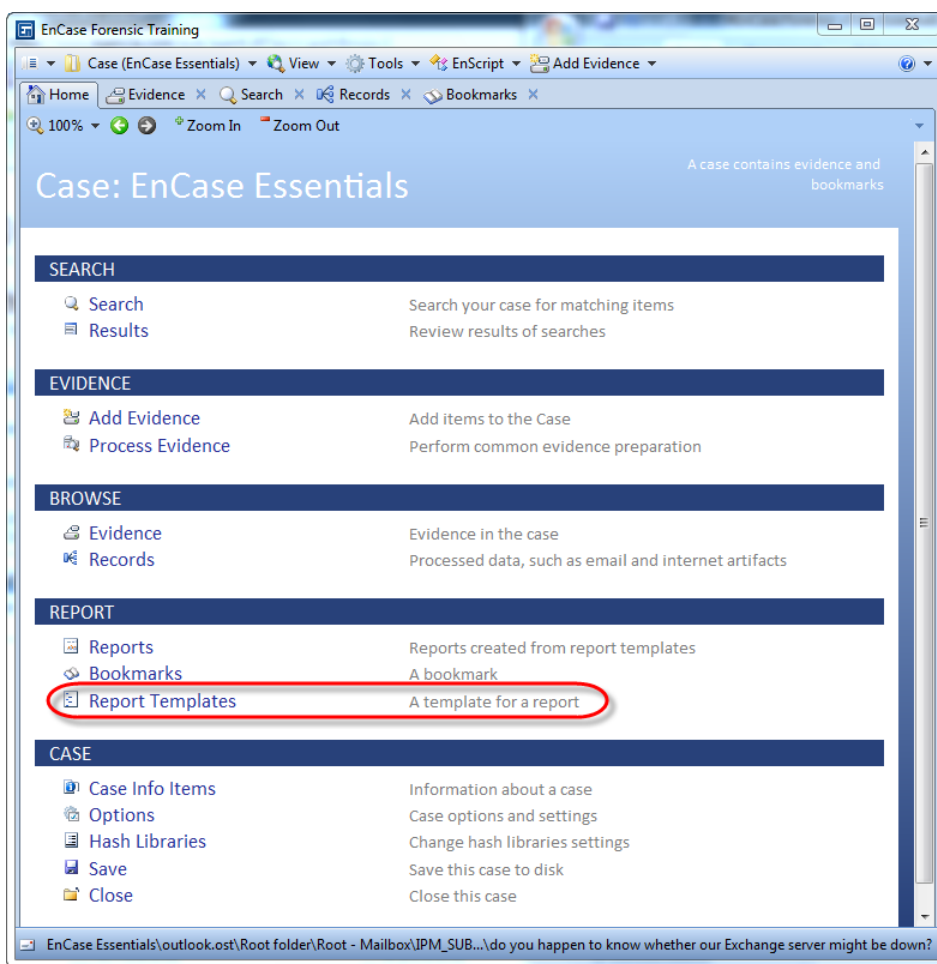
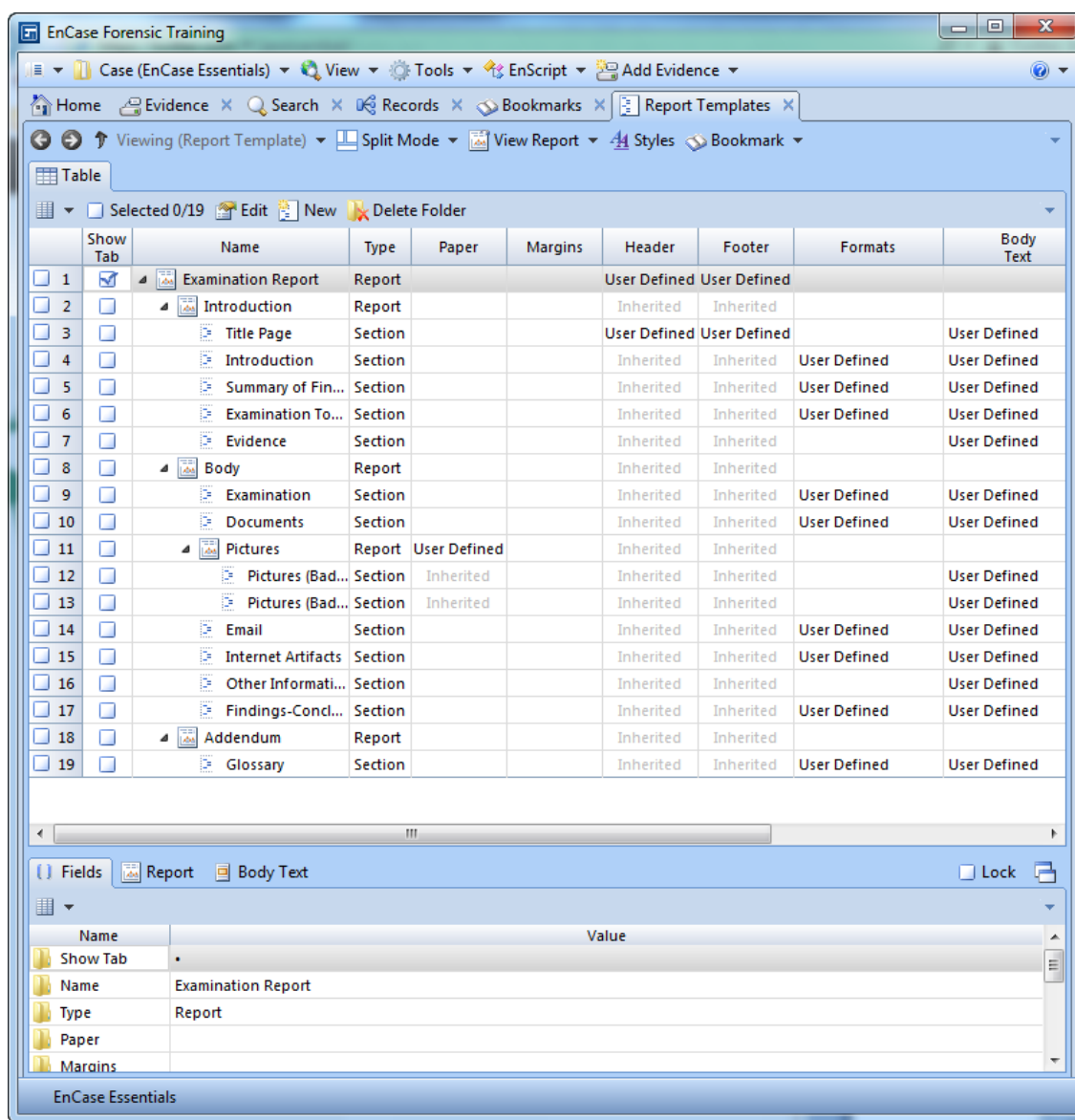


Figure 10-1 Report Templates

Following is an example of the Forensic report template (**Report Templates→Table**).

For organization and flexibility in reporting, a report component can be designated as either a *Report* or *Section*, as shown in the **Type** column of each Table row. Report components typically only contain formatting information for components beneath them, while section components contain formatting information and report elements.

The columns to right of Type indicate whether a particular formatting option is user-defined or inherited from the report or section above it in the hierarchy of rows.



	Show Tab	Name	Type	Paper	Margins	Header	Footer	Formats	Body Text
1	<input checked="" type="checkbox"/>	Examination Report	Report			User Defined	User Defined		
2	<input type="checkbox"/>	Introduction	Report			Inherited	Inherited		
3	<input type="checkbox"/>	Title Page	Section			User Defined	User Defined		User Defined
4	<input type="checkbox"/>	Introduction	Section			Inherited	Inherited	User Defined	User Defined
5	<input type="checkbox"/>	Summary of Fin...	Section			Inherited	Inherited	User Defined	User Defined
6	<input type="checkbox"/>	Examination To...	Section			Inherited	Inherited	User Defined	User Defined
7	<input type="checkbox"/>	Evidence	Section			Inherited	Inherited		User Defined
8	<input type="checkbox"/>	Body	Report			Inherited	Inherited		
9	<input type="checkbox"/>	Examination	Section			Inherited	Inherited	User Defined	User Defined
10	<input type="checkbox"/>	Documents	Section			Inherited	Inherited	User Defined	User Defined
11	<input type="checkbox"/>	Pictures	Report	User Defined		Inherited	Inherited		
12	<input type="checkbox"/>	Pictures (Bad...	Section	Inherited		Inherited	Inherited		User Defined
13	<input type="checkbox"/>	Pictures (Bad...	Section	Inherited		Inherited	Inherited		User Defined
14	<input type="checkbox"/>	Email	Section			Inherited	Inherited	User Defined	User Defined
15	<input type="checkbox"/>	Internet Artifacts	Section			Inherited	Inherited	User Defined	User Defined
16	<input type="checkbox"/>	Other Informati...	Section			Inherited	Inherited		User Defined
17	<input type="checkbox"/>	Findings-Concl...	Section			Inherited	Inherited	User Defined	User Defined
18	<input type="checkbox"/>	Addendum	Report			Inherited	Inherited		
19	<input type="checkbox"/>	Glossary	Section			Inherited	Inherited	User Defined	User Defined

Figure 10-2 Report Template

To add new reports or sections to the template:

1. Highlight the row above the new element that you want to add
2. Click **New...** on the Table tab

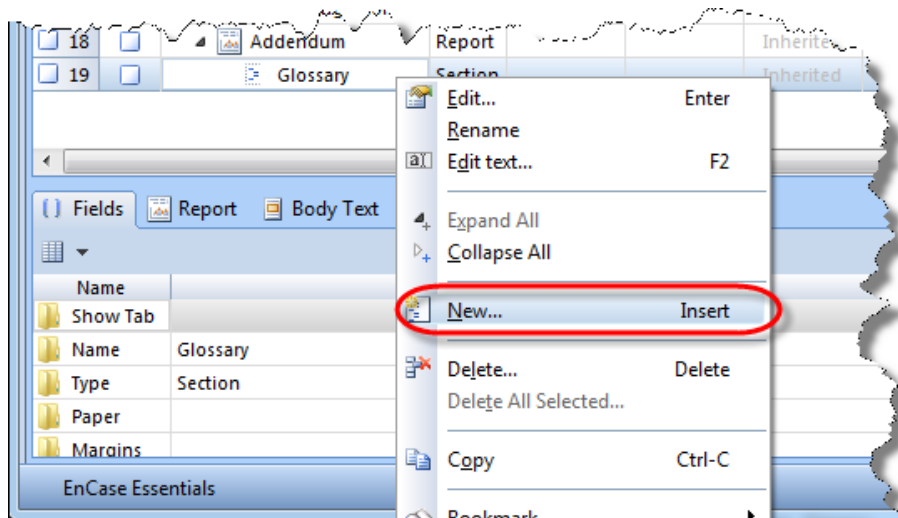


Figure 10-3 New Report template

3. The New Report Template dialog appears

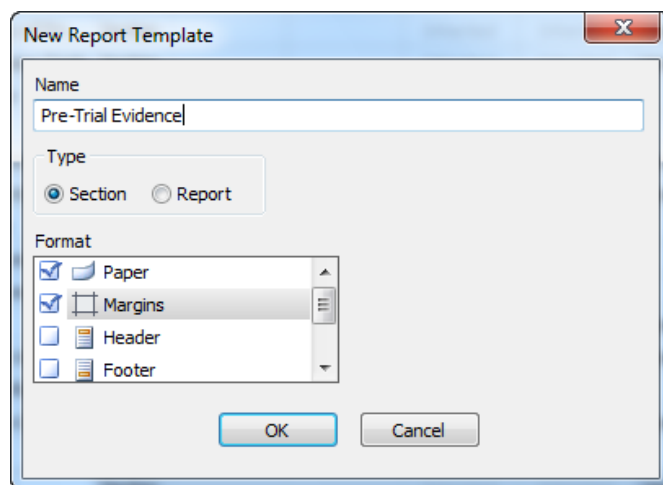


Figure 10-4 New Report Template dialog

4. Type a **name** for the new report template component
5. Select a **type (Section or Report)** for the new template component
6. Select whether you want to customize a Format style by checking its box or use the default format style by leaving the box clear
7. Click **OK**

The new template component will appear below the row that you highlighted.

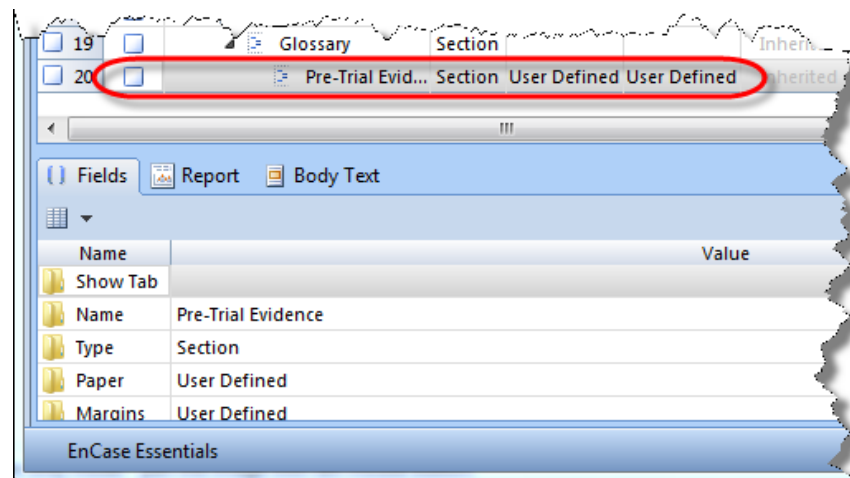


Figure 10-5 New report section

FORMATTING REPORT TEMPLATES

There is a wide range of formatting options available for customizing EnCase v7 reports. Guidance Software recommends using the default case templates as a starting point, such as the Forensic template used in this instruction, and customizing them as necessary. These templates provide examples of most reporting options.

As displayed in the previous screenshots, report templates can and should be designed as a hierarchal tree to simplify formatting. If properly designed, report sections will inherit formatting options from above, therefore, changes to the formatting will only have to be made in one location.

The following is a list of items that can be customized:

- **Section Name** – This name is for organizational reference in the template only and does not populate into the report
- **Paper** – This includes orientation and size
- **Margins** – Values can be set for top, bottom, left, and right margins
- **Header/Footer** – You can design a completely customized header or footer that contains Case Info Items and other various data
- **Data Formats** – The display characteristics of each bookmark type can be customized; this includes data style and content
- **Section Body Text** – The layout and content of each section is specified in the Body Text
- **Show Tab** – This options determines if this report or section is displayed as a tab in the Reports tab
- **Excluded** – Provides the ability to quickly exclude a section from a report if it is not applicable

Editing a Formatting Option

To edit a formatting option:

1. Right-click on a cell that represents the report element and the formatting component you want to edit
2. Click **Edit...** on the cell's context menu
3. Change the default values for the formatting option to the values you want
 - In the following example, the Margins cell for the Body element is selected and the left and right margins are changed from the default values to one inch

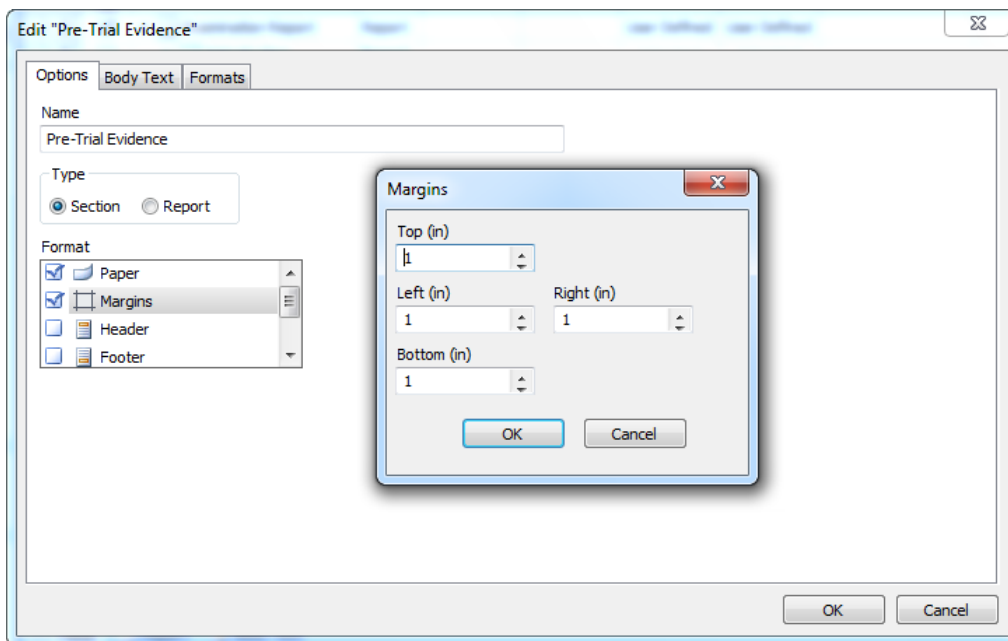


Figure 10-6 Report Margins

4. Click **OK** when you are finished

NOTE: Remember formatting options, from beginning to end, are inherited by default. Therefore, in this example, the margins for the report components that follow the one you customized will inherit those margin settings unless you edit them.

REPORT STYLES

As in Microsoft Word, styles are used to set text formatting options. EnCase v7 comes with many default styles that can be used in report templates and you can create your own styles. You can override a default style by creating a user style with the same name.

Options that can be designated in a style include:

- Font type and font size
- Alignment (left, center, right, justified)
- Indenting (left, right, first line)
- Space before/after
- Borders
- Tabs
- Text color
- Background color

To Create a User-defined Style

From the Report Template tab, select **Styles** from the Tab toolbar.

A new window appears that contains a tab for **Default Styles**, which displays the available default styles, and a tab for **User Styles**:

1. Switch to the **User Styles** tab

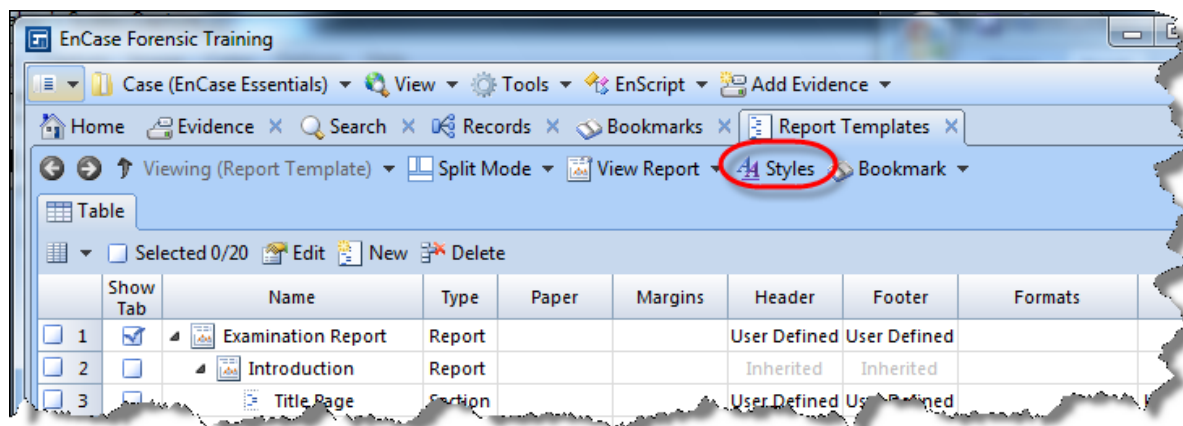


Figure 10-7 Styles

2. Select **New** from the toolbar

- The ability to edit or delete an existing user style can also be found in the toolbar

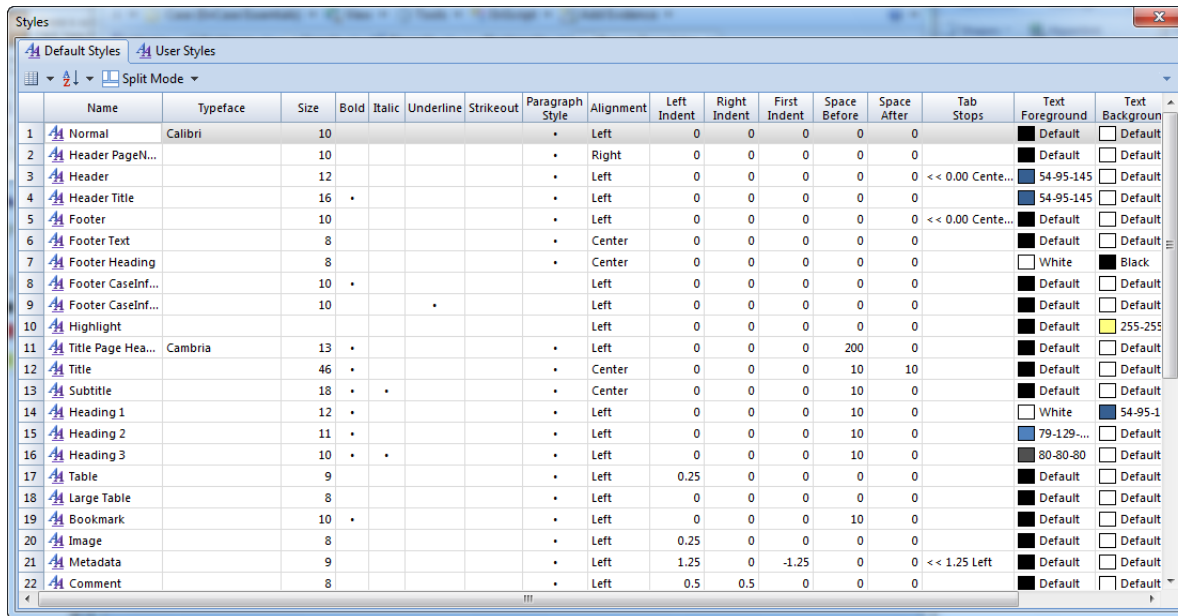


Figure 10-8 User Styles

3. Provide a name for the style and desired configuration options

- Font, Text Foreground, and Text Background can all be set by double-clicking on the appropriate field

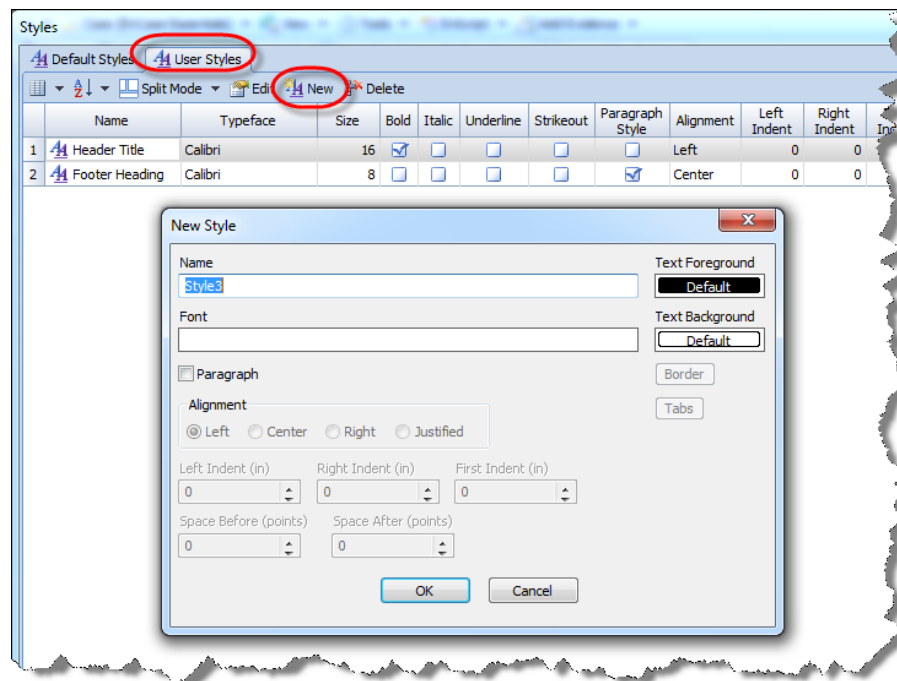


Figure 10-9 New user style

VIEWING A REPORT

Once you have configured your report template and added bookmarks to the appropriate folders, there are two ways to view a report:

1. From the Report Templates tab, select **View Report** from the tab toolbar
 - This will list all reports that have the Show Tab option set
 - Selecting a report from the menu takes you to the Reports tab to view the selected report

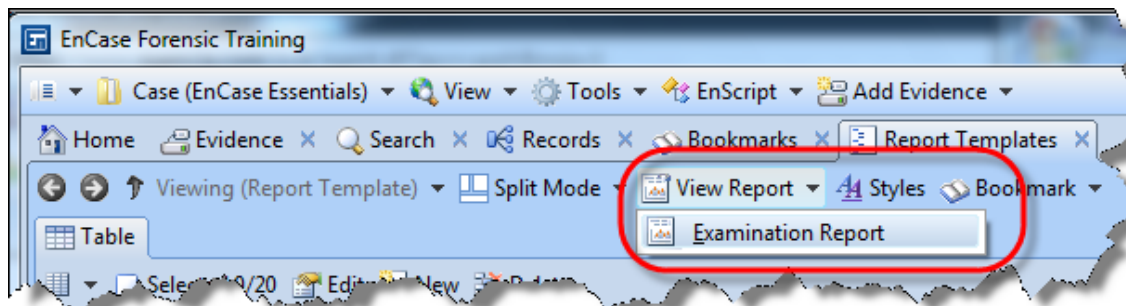


Figure 10-10 View Report

2. You can also select the **Reports** tab from the case Home page or the View menu
 - In the Reports tab you will see a tab for each report that has the Show Tab option set

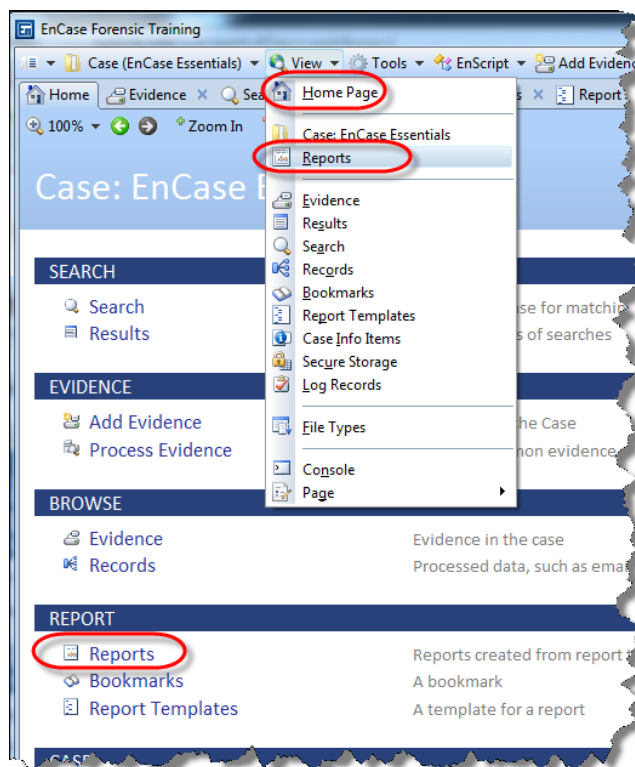


Figure 10-11 Reports

Reports are dynamically generated every time that you switch to a specific report in the Reports tab. To save a report, right-click on the report and select **Save As**. The following output formats are available:

- TEXT
- RTF
- HTML
- XML
- PDF

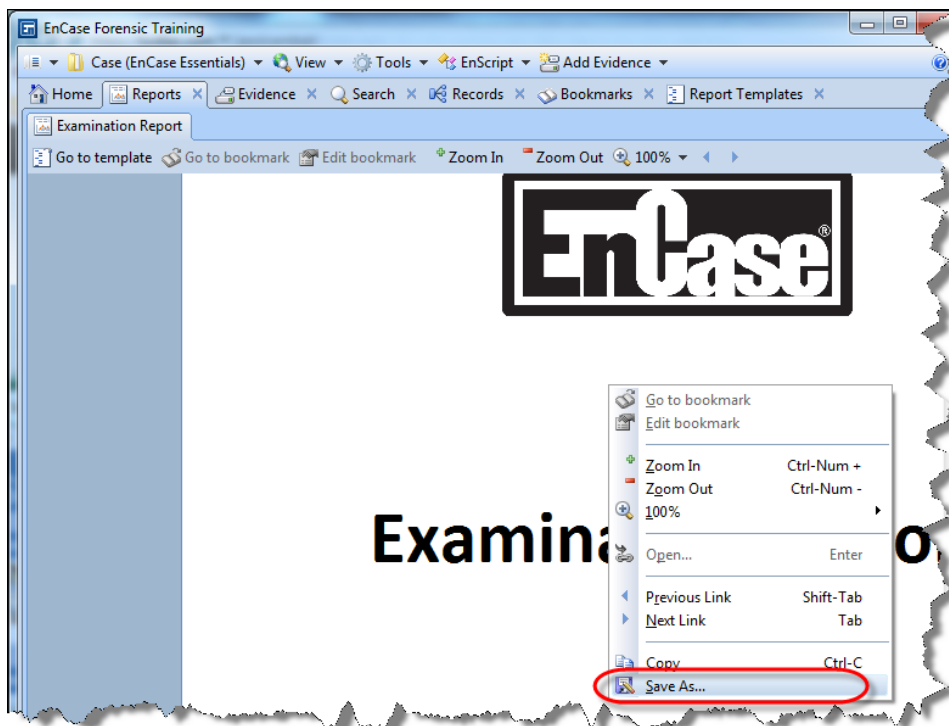


Figure 10-12 Save the Report

Once you select the output format, specify a **Path** and optionally set the **Open file** option if you want the file to open in the default application after saving.

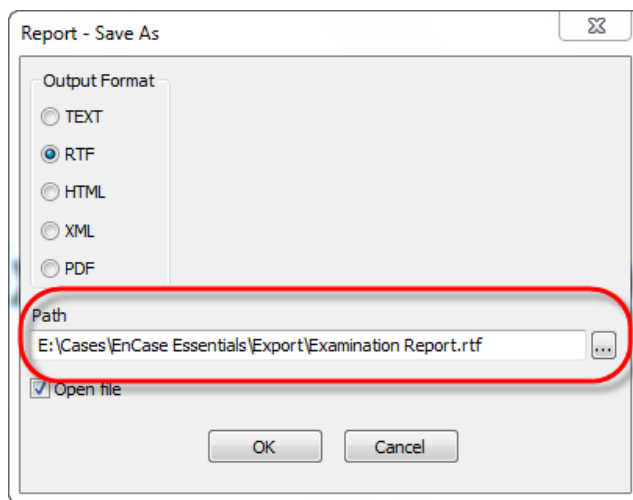


Figure 10-13 Output Format

NOTE: It is recommended that if you wish to edit your report in Microsoft Word, you save the report in RTF format. The EnCase® RTF report is completely compatible with Microsoft Word.

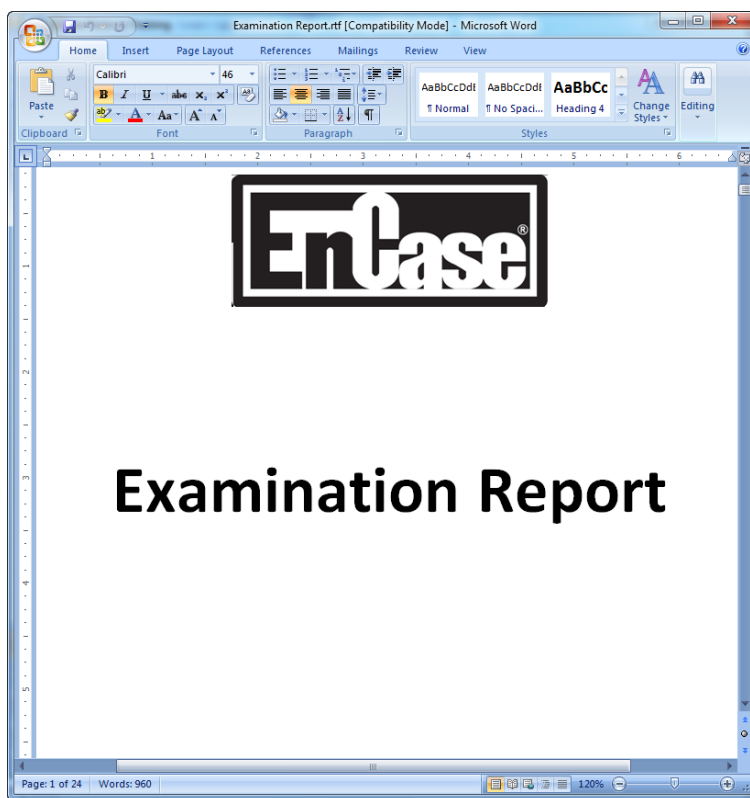


Figure 10-14 Report open in Microsoft Word

CASE ARCHIVING AND PORTABILITY

Cases in EnCase v7 have a significant amount of user data stored in the evidence cache and files other than just the .case file itself. You may need to package up your evidence and case and move or share it between multiple users.

The new case packaging feature in EnCase v7 allows you to package up all of the relevant items associated with a case and put them in a single folder for archiving or case portability.

In the Case menu, select **Create Package**.

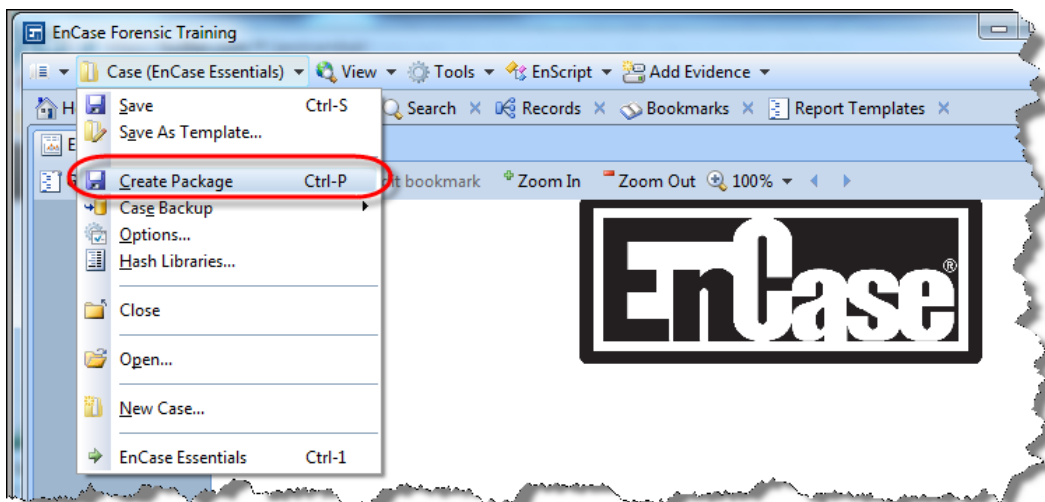


Figure 10-15 Create a Case Package

The Create Package interface will appear with packaging options:

- **Copy** – Copy the case file, evidence cache(s), and other required files for case portability between examiners
- **Archive** – Archive the case file, evidence cache(s), other required files, and the evidence files of the case
- **Customize** – Choose what files to package

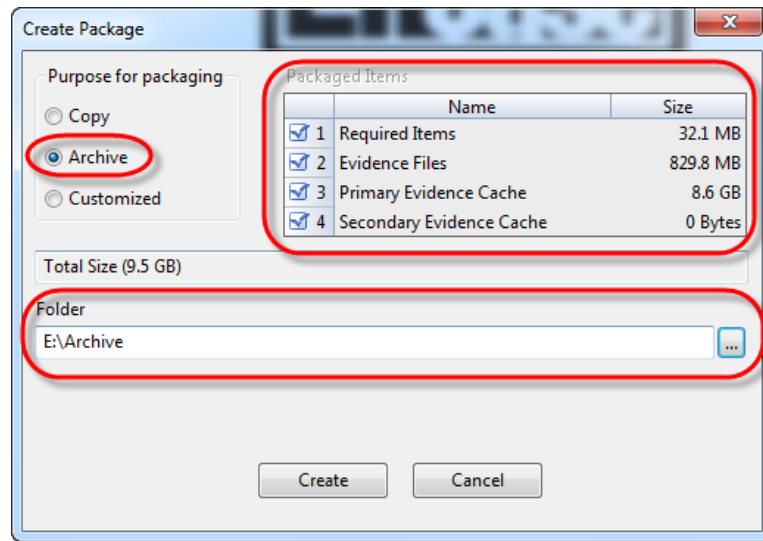


Figure 10-16 Create Package options

The case information is displayed, including:

- Current case name and location
- Size of required items
- Size of optional items
- Total size

The Create Package options include:

- Target location to save the case package
- Checkbox for evidence files (only if items exist and are available)
- Checkbox for Primary Evidence cache items (only if items exist)
- Checkbox for Secondary Evidence cache items (only if items exist and primary is selected)

When the data is backed up to the target folder each evidence file or file set will be put into its own subfolder. A progress bar will show you the percentage complete.

[illegible]

[illegible]

[illegible]

Appendix A – Index Queries

CREATING A SEARCH QUERY

Once your case has been indexed, keyword searched, tagged, or any combination of the three, you can then search for desired information. To create a unified search do the following:

1. Go to the **Home** screen and click the **Search** button

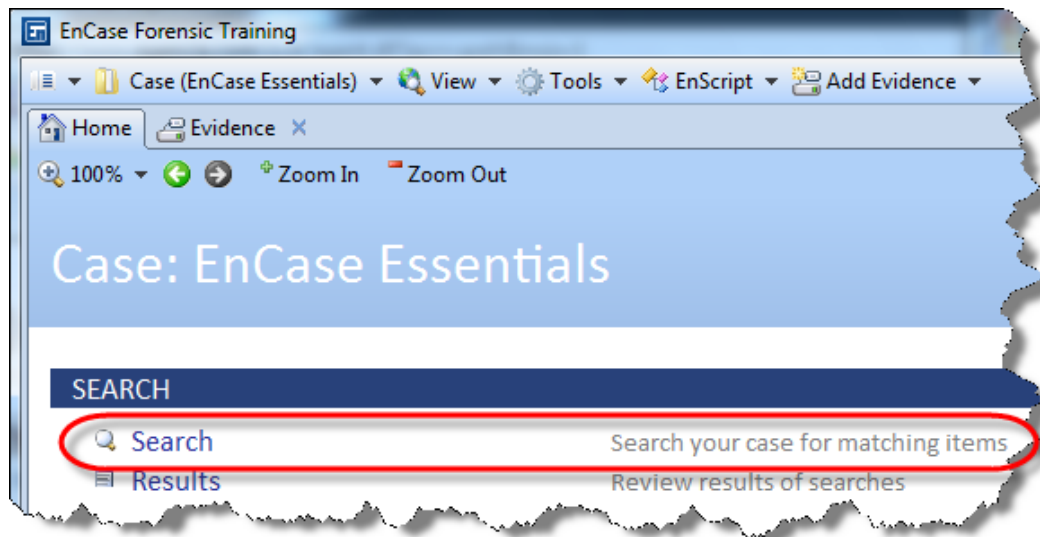


Figure 11-1 New Search...

2. In the Index window, enter the keyword(s) to query the index, such as "Tyler"
3. A dynamic list is displayed on the right side of the window, showing the terms in the index and the number of occurrence of a term; this is extremely helpful when crafting a query so that you can immediately see if the term exists in the index.
4. EnCase v7 will show you all words in the index that start with the term that you have typed and will dynamically update the list as you type additional letters; at any time you can double-click on a query term and it will show the information about that term

5. Click on the **Play** button to run the query

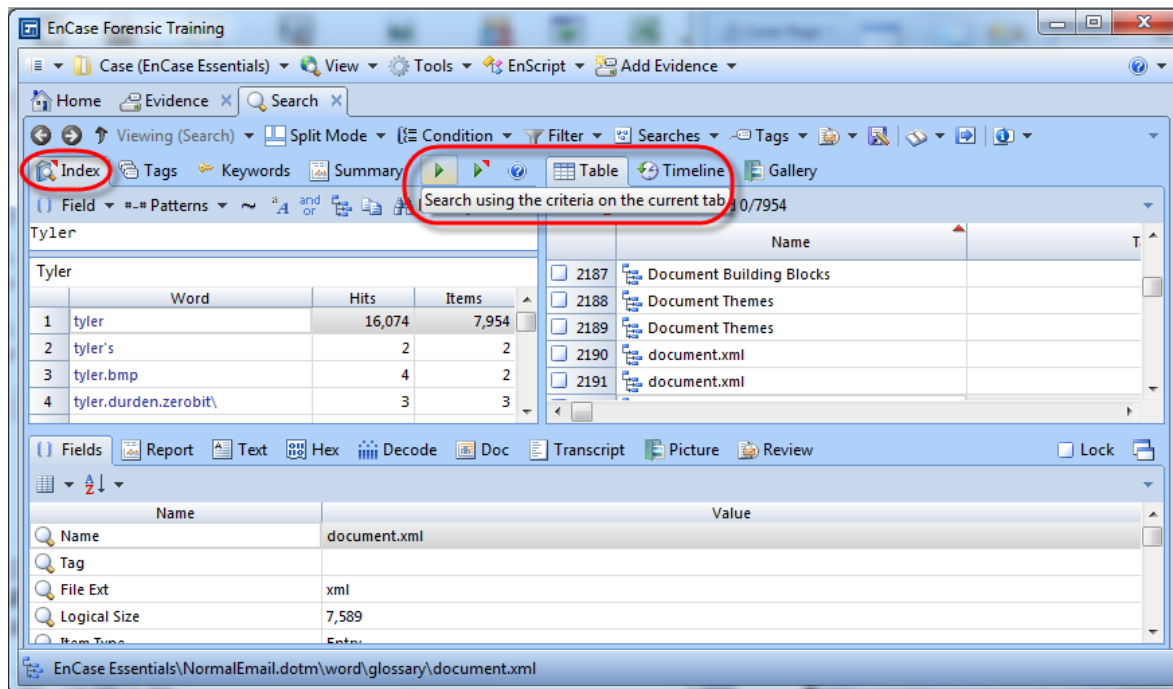


Figure 11-2 New Search interface

Search New

By default, EnCase v7 searches for items containing all the keywords in the search term. For instance, the search term "George Washington" searches for all items that contain both the word "George" and the word "Washington:"

- You can search for documents containing either keywords by using the OR operator, e.g., George OR Washington
- You can use the AND operator for clarity, e.g., George AND Washington

However the latter term produces exactly the same results as the original search term.

Proximity

To search for two keywords within a specified number of words from each other, use the **w/** operator:

- George w/3 Washington
- Abraham w/5 Lincoln

One Word before Another

You can also search for documents where the first keyword precedes the second by no more than a specified number of words:

- George pre/3 Washington
- Abraham pre/3 Lincoln

Keywords Apart From Each Other

To search for documents where the keywords are *not* within a certain number of words of each other, use the **nw/** or the **npre/** operators:

- George nw/3 Washington
- Abraham npre/3 Lincoln

Exact phrases

You can search for exact phrases using quotation marks (""), which is the same as using the **pre/1** operator:

- "George Washington" is the same as George pre/1 Washington

Near the Front or End of the Document

You can use the reserved words "firstword" and "lastword" with the proximity operators to refer to the beginning or end of the document. For example:

- George w/3 firstword
 - Finds documents where George is one of the first three words in the document, and
- Washington nw/20 lastword
 - Finds documents where Washington is not any of the last twenty words in the document

With Two Variables

Use parentheses to group multiple words within a search term. For example in the following search term:

- Bill w/5 (Clinton or Gates)

The index marks as responsive all items containing the word “Bill” within five words of either Clinton or Gates.

With Multiple Variables

You can also construct a complex proximity search that includes Boolean operators on both sides. For example in the following search expression:

- (Bill and William) w/5 (Clinton and Gates)

The index marks as responsive all items that contain both the words “Bill” and “William” within five words of both Clinton and Gates.

Grouping Search Queries Together

You can group search queries together using parentheses to form logical expressions. How you use parentheses indicates to the search engine the order in which it should look for the search terms. For instance:

- (George and Washington) or (Abraham and Lincoln)
 - Finds all items with either both the words “George” and “Washington” or both the words “Abraham” and “Lincoln”

You can nest parenthetical expressions; for example:

- (George and (Washington or Bush))
 - Finds all items that contain the word “George” and either the words “Washington” or “Bush”

Alternatively,

- (George and Washington) or Bush
 - Finds all items that contain the words “George” and “Washington,” or “Bush”

You can use parentheses to join proximity queries (pre/, w/) to Boolean logic queries (AND, OR). For example,

- Delaware and (George pre/3 Washington)
 - Finds all items that contain the word “Delaware” and that also contain the word “George” no more than three words before Washington

You cannot use parentheses to put a Boolean term into a proximity term:

- ***Disallowed:*** George pre/3 (Washington and State)

Instead, express this term as follows:

- (George pre/3 Washington) and (George pre/3 State)

Searching for Keywords in Document or E-mail Fields

By default, EnCase v7 searches for keywords in every indexed text field of the document or e-mail. You can restrict the fields that you search using the bracket ([]) field specifier. For instance, to search only for keywords in the subject line, use:

- [Subject]George

You can use parentheses to group keywords together within a field:

- [Subject](George Washington)
- [Subject](George pre/2 Washington)

You can use aliases to group together a section of fields:

- [Address] searches the [To], [From], [CC] and [BCC] fields
- [Date] searches the [Accessed], [Created], [Modified], [Written], [Sent] and [Received] fields

Common fields for all items are:

- [Name]Name of file.File extension (the file will not be found unless it contains the extension)
- [Extension]File extension
- [Category]Category of file, such as Picture

Searching for Date Fields or Date Properties

You can search for items by date or date range using field syntax. Dates are entered in ISO 8601 syntax between # marks and can be general, such as:

- [Created]#2004#

Or very specific:

- [Created]#2004-11-19T11:54:03#

You can also search for date ranges using an ellipsis (...):

- [Created]#2004-02-03...2004-02-17#

The previous term searches for any item with a creation date between Feb. 03, 2004 and Feb. 17, 2004. You can search for items before or after a particular date by leaving off one end of the range:

- [Created]#2004-02-03...#
- [Created]#...2004-02-17#

File date fields are:

- Accessed
- Created
- Modified
- Written

E-mail date fields are:

- Sent
- Received
- Created

Searching for Numeric Properties

You can search for items by number range using field syntax. Numbers are entered between # marks and can be specific, such as:

- [Size]#1034# Analyzing Collected Data 355

Or a range, using ellipses, such as:

- [Size]#1000...3000#

The previous term searches for any item with a size between 1000 bytes and 3000 bytes. You can search for numbers above or below a particular point by leaving one end of the range off:

- [Size]#...3000#
- [Size]#1000...#

Searching for Case-sensitive Terms

By default, all index queries are case-insensitive. You can make queries case-sensitive by using the <c> operator:

- <c>George
- <c>(George and Washington)

You can specify case-sensitive queries for fields:

- <c>[subject](George pre/3 Washington)

Using Wildcards to Search for Patterns

You can search for incomplete words or word prefixes using the ? and * operators.

Wildcard for single characters

The ? operator stands as a placeholder for any single characters. For instance,

- c?t
 - Results in hits for documents containing “cat,” “cot,” and “cut,” but not “caught”

Wildcard for multiple characters

The * operator stands as a placeholder for any number of characters. For instance,

- ind*
 - Results in hits for documents containing “indecisive,” “indignant,” and “Indiana”

Multiple wildcards

A keyword may contain multiple wildcards (either * or ?), but may not contain wildcards at both the beginning and end of the word. For instance,

- ind*ia*a
- c?t?
- *fi?y
 - Are valid keywords

However:

- *india*
- ?cat?
- *fish?
 - Are not valid keywords

Using wildcards with punctuation

The wildcards ? and * only work for the following punctuation types:

- Dash (-)
- Underscore (_)
- Period (.)
- Comma (,)
- At symbol (@)
- Apostrophe (')

NOTE: Punctuation characters will not be found using wildcards if they are at the beginning or end of words.

Using Stemming Lists to Search for Similar Words

You can use the stemming operator (~) to search for similar words. By default, the stemming operator replaces your word with all words similar to it in the English language. For instance:

- swim~
 - Results in hits for documents containing "swim," "swim's," "swimming," "swam," "swum," etc. Stemming uses the language packs on the server to find words similar to your original term.

When you test your term, a stemming list is added to the term. Stemming lists are contained within the <> characters and clearly display the stems for the keyword. For instance, the default stemming list for swim is:

- <s:swim swim's swims swims' swimming swam swum swim>

You can override the default stemming behavior by modifying the stemming list. For instance:

- <s:swim swam swum>
 - would result in hits for documents containing "swam" and "swum," but not "swimming," "swim's," etc.

You can incorporate stemming into any location for which you would use the OR operator. For instance:

- run~ and [Created]#2002#
- <s:run ran running runner>
 - Results in hits for documents created in 2002 and contain at least one of instance "run," "ran," "running," or "runner"

FIELDS IN INDEX QUERIES

Index queries can be created that target data in specific data fields. By selecting the **Fields** button on the toolbar, you can double-click on a field name and add it to your query. After adding the field name, type the value for which you wish to query. Category, Item Type, and Signature Analysis have sub-menus with their values.

Following is an example of the field chooser.

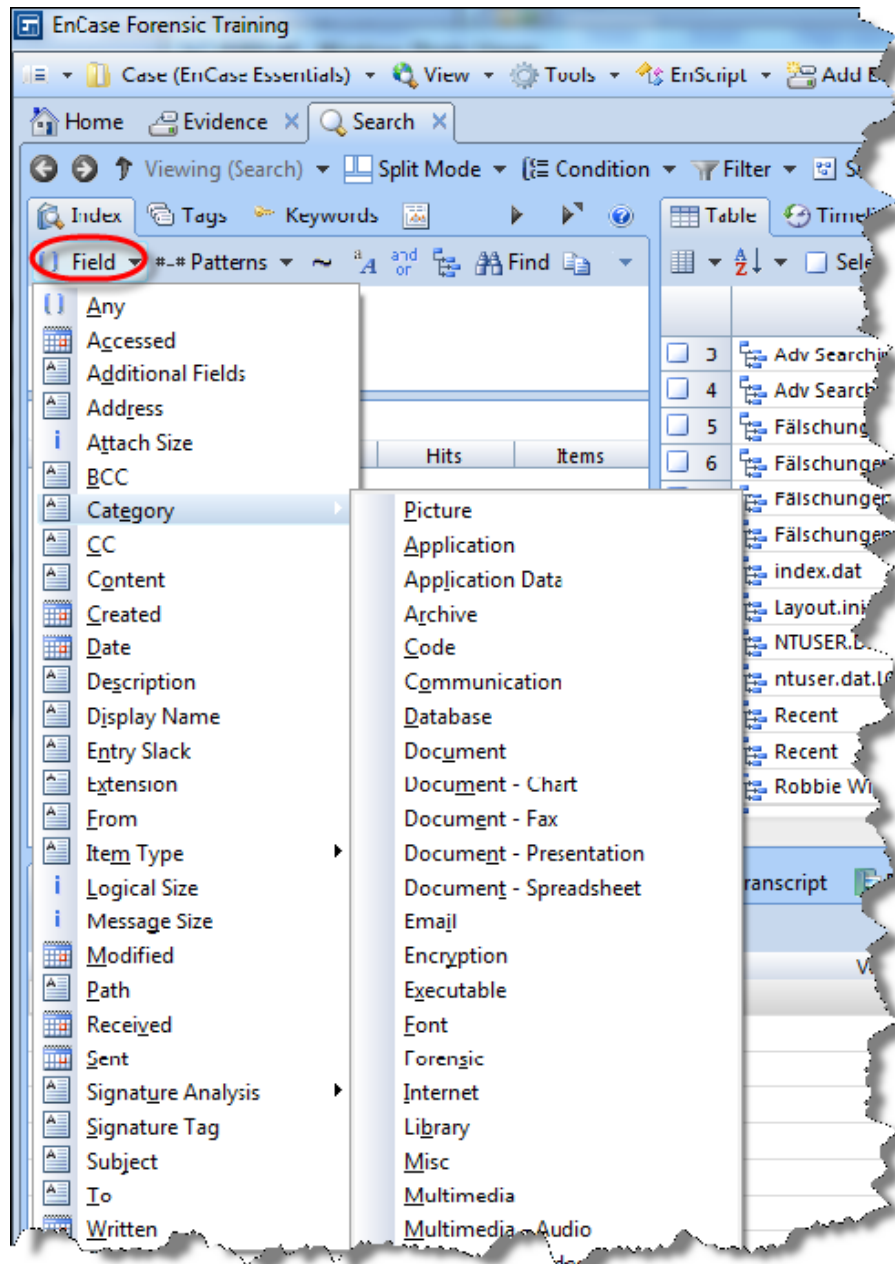


Figure 11-3 Search query field chooser

INDEX QUERY LOGIC

In addition to adding fields into your query, you can also add additional types of logic to customize the result set. The available options are:

- Case sensitivity
- Stemming
- Terms w/ combining logic
- Preview dictionary w/ hit count
- Can combine w/ keyword searches and tags
- Can filter or condition on search results
- Can combine multiple search results w/ and/or logic
- Can view previously run searches

UNIFYING SEARCH RESULTS

EnCase v7 allows you to view search results from a variety of sources, using the single **Search Results** tab. The results can span numerous types of data (for example, files on the Entry tab, e-mail information, and Internet artifacts) and contain the results of a filter, condition, or search (including Index, Keyword, and/or Tags).

All of the operations mentioned previously produce distinct result sets. The queries that are used to display the result sets are stored as files in the users EnCase v7 directory.

Search Result sets can display quickly because they show a subset of available metadata for each item. To view additional information about an item, simply select the item and click **Go to file** in the tab toolbar. The unified metadata available in the Search Results table is:

- Name
 - For an Entry Item: Entry Name
 - For an Email Record: Email Subject
 - For an Internet History Record: URL
- Logical Size
 - Entry: Logical Size
 - Record: Logical Size (PR_LOGICAL_SIZE)

- Last Accessed Date
 - Entry: Accessed
 - Record: Accessed (PR_ACCESSED)
 - Entry: Created
 - Record: Created (PR_CREATION_TIME)
- Last Written Date
- From
 - Email Record: From field
 - Internet History Record: User
- Recipients
 - Email Record: Aggregation of To\Cc\Bcc fields
- Comment
- Item Type
- Category
- Primary Device
- Item Path

The Search Result table displays two additional columns that are dynamically generated based on the items in the table:

- Extension
 - Generated from the Search Result Name at display time
- Tags
 - Generated from the current case at display time

[illegible]